Offensive Cyberspace Operations: Operational Logic, Strategic Utility, and Governance in Contemporary Cyber Conflict

Chuck Easttom
Vanderbilt, Georgetown, and Capitol Technology University, USA

chuckeasttom@gmail.com

Abstract: Offensive cyberspace operations (OCO) have matured into a routine instrument of state power across the spectrum from day-to-day strategic competition to armed conflict. Yet OCO remains unusually difficult to conceptualize and govern because cyberspace is privately owned, technically volatile, and operationally interdependent with civilian critical infrastructure and global software supply chains. This paper develops a doctrinally grounded, technically informed framework for analyzing OCO across tactical, operational, and strategic levels of war while avoiding tradecraft. It models OCO effectiveness as an access-to-effects pipeline constrained by target system dynamism, intelligence requirements, identity and access management (IAM) complexity, tool exposure risk, and the probability of uncontrolled propagation or collateral impact. Empirically, contemporary intrusion data underscores that exploit-driven initial access is common and that remediation timelines often lag adversary tempo, reinforcing the perishable nature of access (Verizon, 2025; Mandiant, 2025). Strategically, OCO can enable campaign disruption, deterrence by denial, and information advantage, but their coercive predictability is limited, and their escalation externalities can exceed those of conventional fires in tightly coupled socio-technical systems. The paper synthesizes public doctrine, national strategies, and contemporary legal debates, emphasizing that credible governance must integrate military, intelligence, diplomatic, and software-engineering risk perspectives, including vulnerability-equities decisions and supply-chain assurance. It further highlights accelerants—AI-enabled capability scaling and the commodification of access through criminal markets—that compress decision timelines and blur state–non-state boundaries. The conclusion proposes a research and policy agenda centered on measuring effects over time, institutionalizing robust review and oversight, and strengthening resilience to manage the distinctive systemic risks of offensive cyber power.

Keywords: Offensive cyber operations, Cyberspace operations, Persistent engagement, Defend forward, Escalation, International law, NATO, Governance, AI-cyber nexus, Underground markets, Cyber-physical risk, Vulnerability equities

1. Introduction

Cyberspace has become a persistent arena of geopolitical contestation in which states and non-state actors continuously probe, exploit, and manipulate information systems to obtain intelligence, impose costs, and shape decision environments. Unlike traditional domains, the cyber domain is constituted largely by privately operated infrastructure and software-defined architectures that change rapidly through patching, configuration drift, container redeployments, identity policy updates, and supply-chain releases. These structural properties create a strategic paradox: cyber operations can project power without physical border crossings, yet the same connectivity that enables action also amplifies systemic spillover risk and the probability of collateral impact on civilian services (Theohary, 2024).

Operationally, modern targets are hybrid by default: enterprise networks fuse on-premises assets with cloud control planes, software-as-a-service (SaaS) tenants, managed identity providers (IdPs), and third-party integrations. The attack surface therefore includes not only hosts and networks, but also API permissions, federated authentication flows, secrets sprawl in CI/CD systems, and shared dependencies such as managed service providers (MSPs). For OCO, this increases both the intelligence burden—accurate modelling of a target's socio-technical configuration—and the governance burden—risk analysis for second-order effects in ecosystems not owned by the target state.

Offensive cyberspace operations differ from kinetic strike operations in ways that matter for both military doctrine and public oversight. Access is perishable; effects can be reversible, non-linear, and difficult to attribute; and operational success often depends on detailed intelligence regarding target configurations, defensive telemetry, and operator-controlled deconfliction (Joint Chiefs of Staff, 2018; Borghard and Lonergan, 2019). These features complicate deterrence signaling, post-operation battle damage assessment, and proportionality analysis. They also produce a persistent asymmetry between the rate of technological change (often days) and the pace of institutional decision processes (often weeks to months).

2. Definitions and Scope

U.S. doctrine frames cyberspace as a global domain within the information environment composed of interdependent networks, information systems, and embedded processors and controllers (Joint Chiefs of Staff, 2018). 'Cyberspace operations' describe the employment of cyberspace capabilities to achieve objectives in or

through cyberspace, including effects that can manifest outside the domain via cyber-physical coupling. Within that doctrinal frame, OCO are operations intended to project power by applying force in or through cyberspace to deny, degrade, disrupt, destroy, or manipulate adversary systems, data, or decision processes (Theohary, 2024).

This paper distinguishes OCO from closely related activity that is often operationally intertwined. Cyber espionage (commonly framed as cyber collection or CNE) seeks information advantage; it may share access pathways and infrastructure with OCO but typically aims for persistence and stealth rather than overt effect. Defensive cyberspace operations (DCO) focus on detection, mitigation, and active defense, while Department of Defense Information Network (DODIN) operations sustain mission networks. In practice, campaigning concepts such as persistent engagement and defend forward intentionally blur these boundaries, emphasizing continuous contestation and pre-emptive disruption of adversary infrastructure (U.S. Department of Defense, 2018; U.S. Cyber Command, 2022; Healey, 2019).

Scope is bound to strategic and operational analysis and explicitly omits tradecraft. Accordingly, discussion focuses on enduring technical constraints, risk dynamics, and governance mechanisms rather than procedural methods for intrusion, exploitation, or tool construction. Where technical terminology is used (e.g., 'control plane', 'EDR telemetry', 'privilege boundary'), it is intended to describe the risk surface and decision variables relevant to policy and command.

3. Policy and Legislative Context

OCO sits at the intersection of military activity, intelligence collection, and domestic legal controls. In the United States, operations may be conducted under military authorities (often associated with Title 10), intelligence authorities (often associated with Title 50), or hybrid arrangements combining intelligence preparation with military execution (Theohary, 2024). This legal geography shapes oversight, reporting, permissible objectives, and the ability to integrate effects with other instruments of national power—especially in the 'below-armed-conflict' space of strategic competition.

Strategic guidance since 2018 has emphasized a proactive posture. The 2018 DoD Cyber Strategy articulated defend forward, while U.S. Cyber Command describes persistent engagement as continuous contestation of adversary campaigns rather than episodic crisis response (U.S. Department of Defense, 2018; U.S. Cyber Command, 2022). The 2023 DoD Cyber Strategy summary similarly frames cyberspace operations as integral to campaigning and integrated deterrence (U.S. Department of Defense, 2023).

Governance also includes decisions about vulnerability retention versus disclosure. The Vulnerabilities Equities Process (VEP) formalizes deliberation over whether to disclose vulnerabilities to improve ecosystem security or retain them temporarily for national security purposes (The White House, 2017; Director of National Intelligence, 2024). In an era of high-tempo patching and 'patch-gap' exploitation, vulnerability policy functions as an operational variable: retention may enable access, but it can also increase systemic risk if the same weaknesses are discovered by adversaries, leaked, or widely exploited.

Table 1: Conceptual distinctions relevant to OCO governance

Activity lens	Primary objective	Typical success metric	Governance emphasis
OCO (effects)	Deny/degrade/disrupt/destroy/manipulate	Operational effect + controllability	Legal review + collateral/spillover risk
Cyber espionage (collection)	Information advantage	Persistence + exfil integrity	Counterintelligence + source protection
DCO	Defend systems and missions	MTTD/MTTR reduction	Resilience + incident response authority
DODIN ops	Network readiness and availability	Service uptime + compliance	Configuration control + supply-chain assurance

4. Analytical Approach: An Access-to-Effects Model

A useful analytic model must connect capability generation, operational employment, and strategic meaning. This paper adopts an 'access-to-effects' abstraction in which OCO are pipelines that convert privileged access into operational effects. Under this model, access is a perishable asset subject to detection, patching, credential

rotation, and architectural change; effects are contingent outcomes mediated by socio-technical systems, including automated defenses and organizational resilience (Healey, 2019; Borghard and Lonergan, 2019).

The model highlights a practical reality: many OCO failure modes occur before any payload-like mechanism is relevant. Failures include mis-modelled identity topologies, unanticipated cloud policy constraints, EDR detections at the telemetry layer, or the loss of an access pathway due to routine maintenance. The access-to-effects approach therefore treats intelligence preparation of digital terrain as analogous to weaponeering: operators must characterize dependencies, identify 'choke points' in workflows, and estimate the reliability and reversibility of potential effects.

Formally, the expected utility of an OCO action can be expressed as an engineering-style risk trade: EU ≈ P(access) × P(effect|access) × Value(effect) − [Risk(exposure) + Risk(spillover) + Risk(escalation)] × Cost. This is not a predictive equation so much as a decision framework: it forces explicit assumptions about probability, value, and externalities that can be challenged in review and oversight.

5. Operational Logic and Technical Constraints

The decisive factor in many OCO is not 'payload sophistication' but the fidelity of target system understanding. Contemporary environments integrate cloud services, identity and access management layers, software-defined networking, endpoint telemetry, and third-party dependencies that can change faster than a cyber operation's planning cycle. Configuration drift, patching, certificate rotation, and CI/CD deployments can invalidate assumptions and collapse access windows. Consequently, OCO are increasingly shaped by operational tempo and logistics—maintaining access in a moving target—rather than a one-time technical breakthrough.

Incident telemetry supports this access-centric framing. The 2025 Verizon Data Breach Investigations Report (DBIR) analyzed 12,195 data breaches across 139 victim countries, and found that credential abuse (22%), exploitation of vulnerabilities (20%), and phishing (16%) were leading known initial access vectors in non-error, non-misuse breaches (Verizon, 2025). The same report notes that perimeter device vulnerabilities were fully remediated only about 54% of the time, with a median of 32 days to complete remediation—an interval that can be operationally significant when adversaries pursue rapid exploitation (Verizon, 2025).

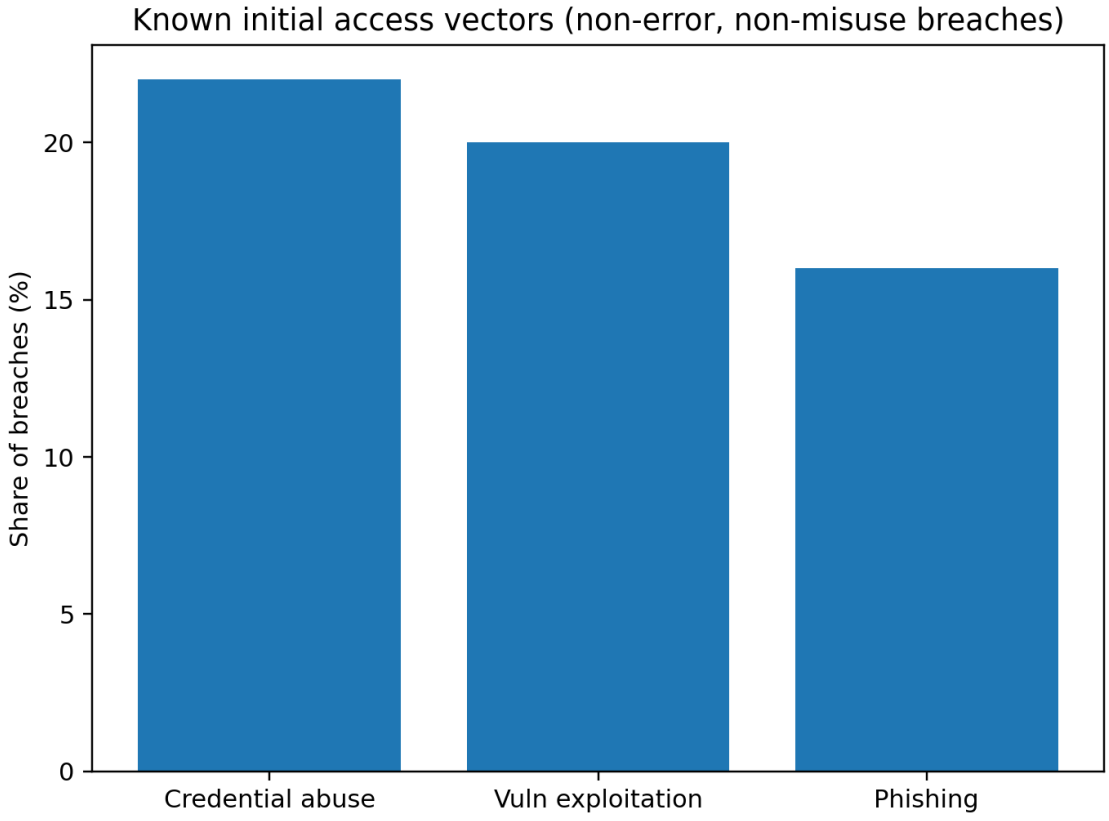

Figure 1: Known initial access vectors reported in Verizon DBIR 2025 (values shown are percentages). Source data: Verizon (2025)

From an operational perspective, the access-to-effects pipeline typically traverses multiple trust boundaries: external perimeter to identity plane, identity plane to workload plane, and workload plane to data plane. Each boundary introduces distinct defensive controls (e.g., MFA and conditional access at the identity layer, EDR and application allow-listing at endpoints, policy enforcement at cloud APIs). Maintaining operational security requires minimizing distinctive artifacts, managing observables, and deconflicting with other operations. Repeated use of a capability increases exposure risk, enabling defenders to detect, attribute, and mitigate, thereby reducing future utility (Borghard and Lonergan, 2019).

Reliability is also constrained by the heterogeneity of targets. Effects that depend on precise timing, specific library versions, or fragile assumptions about business logic can fail silently. Conversely, effects that propagate across shared dependencies—such as common management tooling, authentication services, or update channels—can exceed intended scope. For governance, this means technical review must include explicit 'blast radius' estimation and fail-safe considerations, not merely legal analysis.

Table 2: Access-to-effects pipeline and common constraint categories

Pipeline stage	Key artefacts	Constraint driver	Typical failure mode	Governance concern
Access establishment	Initial foothold, credentials/tokens	Patch gap; identity controls	Access burned by detection/rotation	Exposure risk; proportionality of entry
Privilege/positioning	Privileges, roles, trust relationships	IAM complexity; segmentation	Blocked by least privilege or policy	Deconfliction; scope creep
Persistence	Automation, renewal paths	Change management; monitoring	Breaks during updates/maintenance	Long-term systemic risk
Effect delivery	Triggers, dependencies, workflows	Target dynamism; safety constraints	Effect partial/reversible/unreliable	Controllability; civilian impact
Assessment & mitigation	Telemetry, restoration signals	Attribution ambiguity; IR maturity	Effects unmeasured or misattributed	Accountability; after-action learning

6. Interdependence and Collateral Effects

Cyberspace interdependence is a structural property of modern digital systems: societies share software stacks, hardware supply chains, managed service providers, and global routing and naming infrastructure. Offensive actions can therefore generate second- and third-order effects through shared dependencies, technical propagation, or operational disruption in adjacent ecosystems. The operational problem becomes one of controlling effects in a complex adaptive system rather than in a closed test environment.

Public attributions of the 2017 NotPetya incident highlight the systemic nature of spillover risk: a campaign aimed at Ukrainian targets rapidly caused widespread disruption and economic harm to global firms (UK Government, 2018; The White House, 2018; CISA, 2017). Such cases illustrate why proportionality and precautions, central concepts in international humanitarian law, must be operationalized as engineering and risk-analysis practices, not treated solely as legal abstractions (Davis et al., 2022; ICRC, 2019).

From a technical risk perspective, collateral pathways include: (1) shared authentication services (IdPs, federation), (2) shared management planes (remote monitoring and management tools, MSP platforms), (3) shared update mechanisms (software repositories and package registries), and (4) shared industrial and critical infrastructure dependencies (OT safety systems and supervisory control networks). Accordingly, resilience engineering—segmentation, redundancy, offline backups, immutable logging, and rapid restoration—functions as a strategic variable shaping both offensive feasibility and defensive survivability.

7. Strategic Purposes and Escalation Dynamics

OCO can support coercion (Fischerkeller, 2022), deterrence, campaign disruption, and information advantage, but these objectives are not equally predictable. Research on cyber escalation emphasizes that cyber operations frequently generate limited and uncertain costs, can be difficult to signal credibly, and often produce non-escalatory patterns of response (Borghard and Lonergan, 2019; Lin, 2012). These features reduce coercive leverage relative to conventional punishment strategies and complicate crisis bargaining.

Persistent engagement logic reframes strategic utility toward deterrence by denial and campaign disruption: continuous interference with adversary cyber capabilities, infrastructure, and enabling resources to impose friction and deny freedom of maneuver (Fischerkeller, 2022; Healey, 2019; U.S. Cyber Command, 2022). OCO can also support information advantage by degrading data integrity or situational awareness in ways that slow adversary decision cycles. Yet such effects may be perceived as escalatory if they threaten strategic stability or appear preparatory to kinetic action, underscoring the need for calibrated signaling and integrated crisis management.

A useful strategic lens is to treat OCO as 'campaign enablers' rather than stand-alone coercive instruments. In integrated operations, cyber effects may shape access to the electromagnetic spectrum, protect force flow, degrade adversary logistics, or contest command-and-control (C2) systems. However, because cyber effects can be transient and rapidly mitigated, campaign planners must consider persistence of effect over time, defender adaptation, and the opportunity cost of capability exposure.

8. International Law and Norms

UN processes have repeatedly affirmed that international law, including the UN Charter, applies to state behavior in cyberspace (UN General Assembly, 2015; 2021; 2023). Operational challenges arise from threshold classification: determining when cyber operations constitute a use of force, when they qualify as an armed attack triggering self-defense, and how to assess scale and effects when harm is economic, informational, or distributed.

States increasingly publish national positions. France emphasizes sovereignty and due diligence as well as the availability of responses under international law (France, 2021). The United States similarly emphasizes that existing international law governs cyber operations and has articulated a 'victim's perspective' focused on harms imposed (Davis et al., 2022; Visek, 2024). Debates persist over the legal content of sovereignty in cyberspace and the precise contours of countermeasures.

During armed conflict, international humanitarian law (IHL) limits cyber operations used as means or methods of warfare. The ICRC stresses that IHL applies fully in cyberspace, including distinction, proportionality, and precautions, and warns that cyber operations can seriously affect civilian infrastructure with potential human harm (ICRC, 2019; ICRC, 2023). Voluntary norms and confidence-building measures endorsed in UN processes aim to reduce misperception and escalation risk, while scholarly restatements such as the Tallinn Manual provide non-binding legal clarification.

9. Alliances and Multinational Cyber Operations

Alliances shape both the feasibility and legitimacy of OCO. NATO has recognized cyberspace as a domain of operations and has affirmed that a cyberattack could, in certain circumstances, trigger Article 5 collective defense commitments on a case-by-case basis (NATO, 2014; NATO, 2023). Nonetheless, NATO emphasizes that offensive cyber capabilities remain primarily national, making coalition cyber effects dependent on sovereign contributions and political authorization.

Multinational coordination is constrained by divergent legal frameworks, political risk tolerances, classification regimes, and technical interoperability. Shared operational pictures may be limited by data-sovereignty concerns and by differing incident response standards. Effective burden sharing therefore includes information sharing, deconfliction mechanisms, and shared risk frameworks for collateral effects—not only investment in capabilities.

10. Governance, Oversight, and Institutional Design

OCO governance must balance operational secrecy, strategic effectiveness, and democratic accountability. Secrecy preserves access and sources, but it limits external scrutiny and can impede institutional learning. Speed increases operational relevance, but it can erode legal review and systemic risk analysis. Accountability requires oversight by elected officials and watchdog institutions, yet the technical and classified nature of OCO creates persistent information asymmetries (Theohary, 2024; U.S. Government Accountability Office, 2025).

Governance frameworks benefit from translating legal and strategic requirements into engineering-style controls: defined risk thresholds, explicit collateral analyses, red-team validation of containment assumptions, and post-operation mitigation plans. A practical approach is multidisciplinary review that combines legal analysis with software-engineering risk assessment (e.g., dependency mapping, 'blast radius' modelling, rollback planning, and verification of restoration).

Broader cyber risk data provides context for why governance must treat spillover seriously. IBM's 2025 Cost of a Data Breach report shows the global average breach cost at USD 4.44 million in 2025, following USD 4.88 million in 2024, and provides a multi-year trend useful for strategic risk framing (IBM, 2025). While the report is not specific to state OCO, it illustrates the magnitude of economic externalities that can arise from cyber incidents and therefore the importance of precautionary controls for operations that could affect civilian systems.

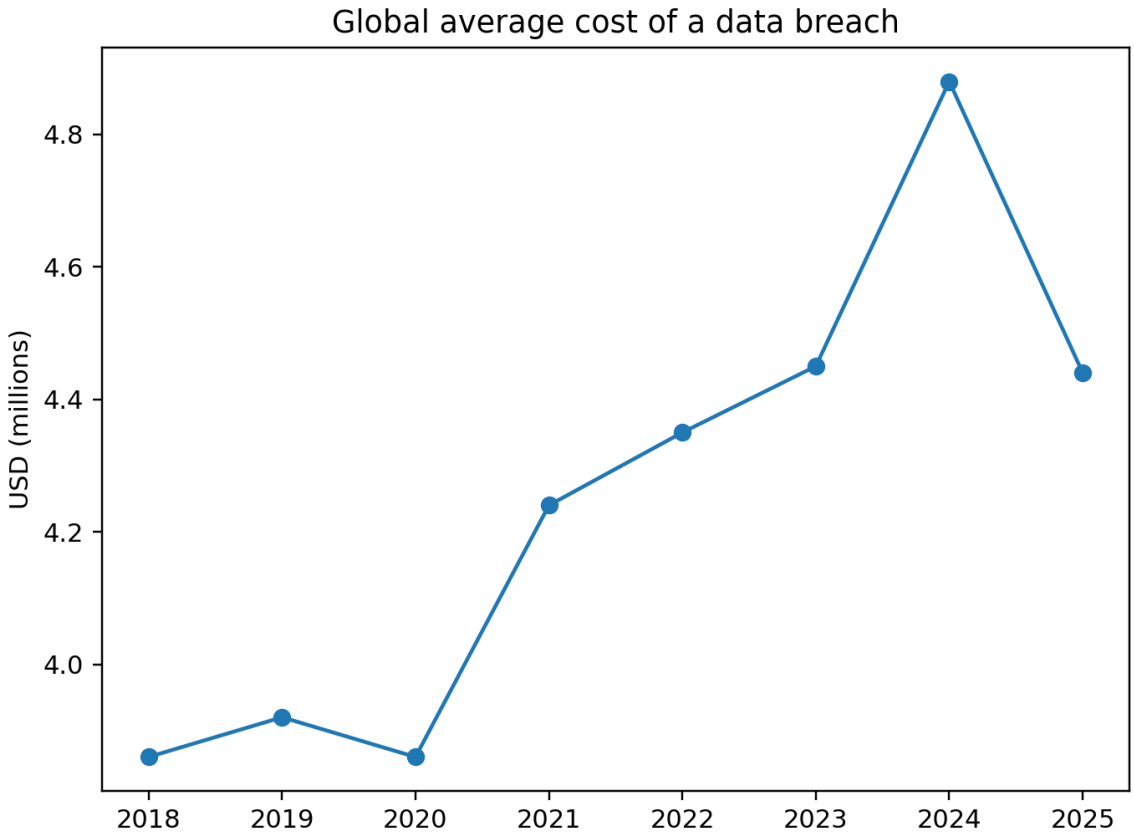

Figure 2: Global average cost of a data breach (USD millions), 2018–2025. Source data: IBM (2025)

11. Measuring Effects: Metrics and Assessment

Measuring OCO effectiveness is difficult because cyber effects are often indirect, mediated by defender adaptation, and confounded by concurrent instruments of power (sanctions, diplomacy, information operations). Unlike kinetic strikes, where crater analysis and sensor logs can approximate immediate physical damage, cyber 'battle damage assessment' may hinge on telemetry access, organizational reporting, and probabilistic inference.

Operational assessment therefore benefits from layered metrics: (1) access metrics (persistence duration, privilege depth, lateral reach), (2) effect metrics (service degradation, data integrity impacts, decision-cycle delays), and (3) externality metrics (spillover indicators, third-party impacts, and exposure costs). For governance, these metrics support after-action learning and provide a defensible basis for proportionality and precaution documentation.

Incident response datasets provide a proxy for the attacker–defender tempo relevant to access perishability. Mandiant reports that exploits were the initial infection vector in 33% of its 2024 investigations, and that global median dwell time rose to 11 days from 10 days in 2023 (still below 16 days in 2022) (Mandiant, 2025). Shorter dwell times can reduce the feasibility of long-horizon access operations, shifting emphasis toward rapid exploitation, automation, and operational security.

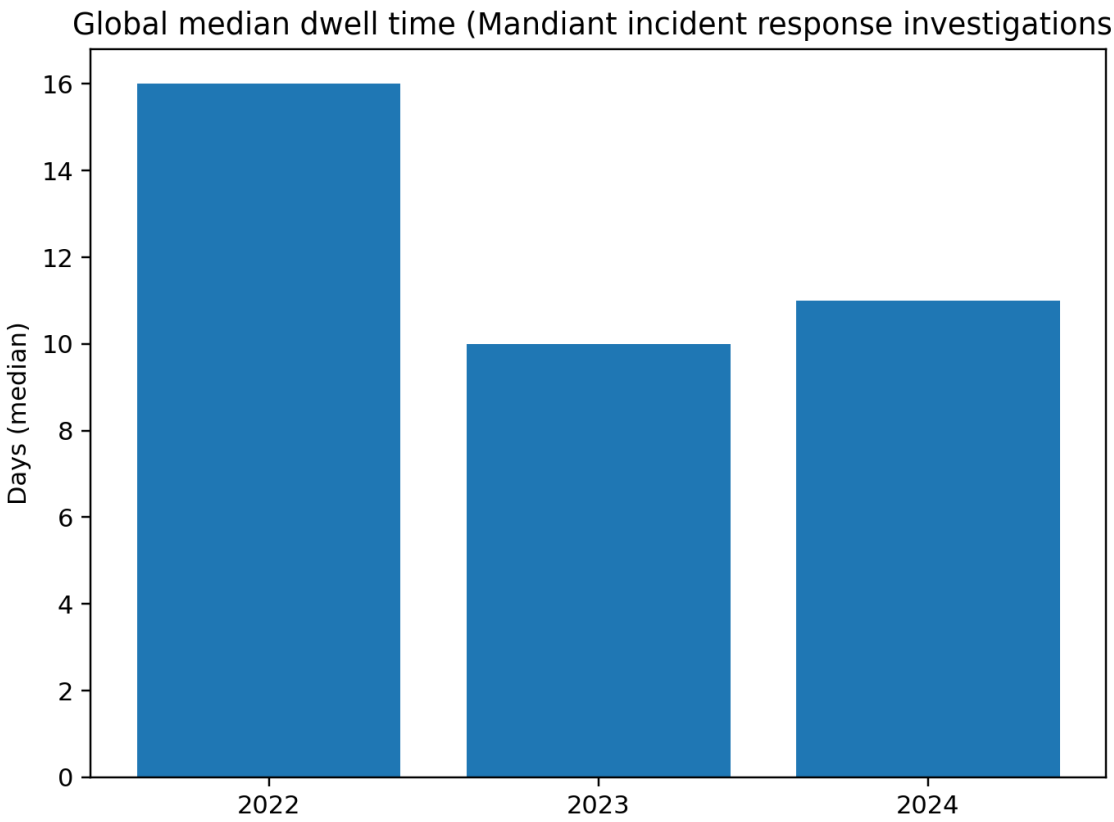

Figure 3: Global median dwell time (days). Source data: Mandiant (2025)

12. Emerging Accelerants: AI-Cyber Nexus and Access Commodification

Two accelerants intensify OCO's operational and governance challenges. First, AI-enabled systems can reduce the marginal cost of reconnaissance, language-specific social engineering, code analysis, and anomaly detection—compressing decision cycles and enabling higher-tempo campaigns. Second, underground markets increasingly commodify access and data through 'initial access brokers' and credential marketplaces, creating a shadow logistics layer for intrusion activity (Europol, 2025).

Recent breach research also points to AI as both an attack multiplier and a governance challenge. IBM reports that 16% of breaches involved attackers using AI, and that 13% of organizations reported breaches involving their AI models or applications; among those organizations, 97% lacked proper AI access controls (IBM, 2025). This suggests that AI systems are emerging as high-value targets and that weak governance—shadow AI, unmanaged plugins, and unreviewed API integrations—can create new pathways for compromise.

At the enterprise boundary, Verizon reports that 15% of employees routinely accessed generative AI platforms on corporate devices, increasing the potential risk for data leakage (Verizon, 2025). For state operators, these trends blur the line between traditional cyber operations and information operations, as AI-mediated influence, credential theft, and data poisoning can intersect with offensive access campaigns.

For governance, the AI-cyber nexus implies that review processes must incorporate model supply-chain risk (plugins, APIs, agents), data residency and privacy constraints, and the possibility of unintended propagation through automated systems. The same logic supports integrating secure-by-design practices, strong identity controls, and continuous monitoring into national cyber posture—reducing incentives to retain vulnerabilities for offensive gain while raising the cost of adversary exploitation.

13. Research and Policy Agenda

Four priorities stand out. First, the field needs rigorous methods to measure OCO effectiveness over time, distinguishing transient disruption from durable degradation and accounting for defender adaptation, restoration timelines, and capability exposure costs. Second, escalation modeling must integrate technical

ambiguity, interdependence spillover, and political crisis dynamics, especially as cyber operations intersect with critical infrastructure and military command systems (Borghard and Lonergan, 2019; Lin, 2012).

Third, policy and research should focus on the AI-cyber nexus and access commodification. AI may accelerate capability generation while introducing new vulnerabilities through autonomous agents and model supply chains; underground markets for initial access and data create a proxy enablement layer that can complicate deterrence and attribution (Europol, 2025; IBM, 2025). Fourth, governance mechanisms should mature toward multidisciplinary review practices that combine legal analysis with software-engineering risk assessment, enabling systematic consideration of collateral effects, long-term systemic vulnerability, and accountable decision records suitable for after-action learning under appropriate oversight.

14. Conclusion

OCO are an enduring element of contemporary state competition and military power, but they are constrained by perishable access, uncertain and interdependent effects, and governance challenges intensified by secrecy and rapid technological change. An access-to-effects model clarifies why OCO require intelligence, engineering rigor, and exposure management as much as technical ingenuity. Strategically, OCO can disrupt adversary campaigns and support deterrence by denial and information advantage, yet escalation and legitimacy risks demand robust oversight and prudent integration with other instruments of national power. As AI-enabled capability scaling and underground commodification accelerate the offense–defense cycle, states and alliances will require disciplined frameworks for risk assessment, legal and normative clarity, and resilience engineering to manage the systemic externalities of offensive cyber power.

Ethics declaration: This research did not involve human subjects and thus no ethical clearance was required.

AI declaration: This research did not use any AI.

References

Davis R. et al, Air Force Cyber Law Primer 2022, https://www.airuniversity.af.edu/AUPress/Display/Article/3209936/air-force-cyber-lawprimer/

Borghard, E.D. and Lonergan, S.W. (2019) 'Cyber Operations as Imperfect Tools of Escalation', Strategic Studies Quarterly, 13(3), pp. 10–38.

CISA (2017) Alert (TA17-181A): Petya Ransomware, US-CERT/CISA.

Director of National Intelligence (2024) FY23 Unclassified VEP Annual Report (Appendix).

Europol (2025) Steal, Deal and Repeat – How Cybercriminals Trade and Exploit Your Data (IOCTA 2025), Publications Office of the European Union.

France (2021) International Law Applied to Operations in Cyberspace, paper shared with the UN Open-ended Working Group.

Fischerkeller, M., Goldman, E. and Harknett, R. (2022) Cyber Persistence Theory. Oxford University Press.

Healey, M. (2019) The Implications of Persistent Engagement in Cyberspace. Oxford: Oxford University Press.

IBM (2025) Cost of a Data Breach Report 2025. IBM Security and Ponemon Institute.

ICRC (2019) International humanitarian law and cyber operations during armed conflicts, Position Paper. Geneva: International Committee of the Red Cross.

ICRC (2023) International humanitarian law and cyber operations during armed conflicts – short papers. Geneva: International Committee of the Red Cross.

Joint Chiefs of Staff (2018) Joint Publication (JP) 3-12: Cyberspace Operations. Washington, DC: Joint Chiefs of Staff.

Lin, H. (2012) 'Escalation Dynamics and Conflict Termination in Cyberspace', Strategic Studies Quarterly, 6(3).

Mandiant (2025) M-Trends 2025: Data, Insights, and Recommendations From the Frontlines. Google Cloud Security.

NATO (2014) Wales Summit Declaration.

NATO (2023) Vilnius Summit Communiqué.

The White House (2017) Vulnerabilities Equities Policy and Process for the United States Government (VEP Charter).

The White House (2018) Statement on the Attribution of the NotPetya Attack.

Theohary, C.A. (2024) Defense Primer: Cyberspace Operations, Congressional Research Service, IF10537.

U.S. Cyber Command (2022) CYBER 101 – Defend Forward and Persistent Engagement.

U.S. Department of Defense (2018) Summary: Department of Defense Cyber Strategy.

U.S. Department of Defense (2023) 2023 Summary of the Cyber Strategy of the Department of Defense.

U.S. Government Accountability Office (2025) DOD Cyberspace Operations: About 500 Organizations Have Roles, with Some Potential Overlap, GAO-25-107121.

UK Government (2018) Foreign Office statement attributing NotPetya to Russia.

UN General Assembly (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174.

UN General Assembly (2021) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/76/135.

UN General Assembly (2023) Advancing responsible State behavior in cyberspace in the context of international security, A/RES/78/16.

Verizon (2025) 2025 Data Breach Investigations Report.

Visek, R.C. (2024) International Law and Cyberspace: A Victim's Perspective, Temple Law Review. https://www.templelawreview.org/lawreview/assets/uploads/2025/01/Visek_International-Law-and-Cyberspace.pdf