THE CYBER DEFENSE REVIEW
In press, 22 pages
https://doi.org/10.55682/cdr/cybr-odc1

RESEARCH ARTICLE

The Offense Death Cycle: Proactive Environmental Control as a Method of Persistent Cyber Defense

Volodymyr Styran*

State Service of Special Communication and Information Protection (SSSCIP), Kyiv, Ukraine

Modern defensive frameworks such as the Cyber Kill Chain, ATT&CK, and D3FEND focus on cataloguing and countering the tactics, techniques, and procedures (TTP) of cyber attackers. While invaluable for incident response, these models remain tactically reactive. In persistent competition, however, Advanced Persistent Threat (APT) attackers and defenders operate in continuous contact within the same contested environment, which renders reactive defensive approaches incomplete. This commentary argues that enduring cyber defense against persistent attackers emerges not from proper reaction but from controlling the environment that the attacker depends on. Building upon Fischerkeller, Goldman and Harknett's Cyber Persistence Theory (CPT), Monte's Network Attacks and Exploitation, and Smeets's PETIO framework, and informed by the author's operational experience, it proposes the Offense Death Cycle (ODC) – a field-informed operational concept for defensive persistence. The ODC translates strategic persistence into a practical loop of intelligence, induced friction, and anticipation, enabling defenders to transform home-field advantage into a source of initiative and to exhaust APTs through executing proactive environmental control.

Keywords: offense death cycle, cyber persistence theory, cyber defense, cyber operations, advanced persistent threat, proactive environmental control, cyber kill chain, att&ck, d3fend, Security Operations Center

* Corresponding author: vlad@styran.com

1 INTRODUCTION: FROM KILL CHAIN TO DEATH CYCLE

The Cyber Kill Chain model (Hutchins, Cloppert, and Amin 2011) and the MITRE ATT&CK framework (MITRE, n.d.) have significantly advanced cyber defense by modeling how attackers operate and making their tactics and techniques observable. They underpin modern detection engineering, threat hunting, and incident response. Yet, by centering on TTPs, these approaches position defenders downstream of attacker initiative. Defenders learn to identify what attackers do, but not why they can keep doing it. MITRE D3FEND, developed as the complement to ATT&CK, maps defensive controls to attack techniques (Kaloroumakis et al. 2021). Still, it inherits the same reactive logic: it prescribes how to mitigate known behavior rather than how to compete for initiative.

What remains largely underdeveloped is a view of cyber defense as a strategic contest unfolding within a shared, contested environment. In modern persistent operations – particularly visible in Ukraine's wartime cyber defense – attackers and defenders coexist continuously in overlapping digital terrain. The environment itself becomes the battlefield, and whoever controls its topology and predictability has the advantage.

Cyber Persistence Theory (CPT) captures this dynamic at the strategic level, framing cyberspace as a domain of continuous great-power competition in which initiative, not deterrence, determines security (Fischerkeller, Goldman, and Harknett 2022). While this perspective has influenced U.S. defense doctrine through the concept of *persistent engagement*, its operational implications remain less clear for enterprise security teams, Security Operations Center (SOC) leaders, and defenders operating outside military command structures. The practical question persists: how can defenders exercise persistent initiative within their own networks?

This article advances a practitioner-oriented answer for SOC leaders, enterprise security architects, and operational defenders seeking a practical way to reclaim initiative against persistent attackers. It grows out of recurring observations in operational environments where routine administrative changes unexpectedly disrupted advanced persistence, and where deliberate environmental manipulation proved more effective than reactive countermeasures alone. These experiences point to a different way of thinking about defense: not as a sequence of responses to attacker actions, but as the continuous shaping of the conditions under which attackers must operate. It does not seek to replace military doctrine or formal strategic theory, but to bridge them with the everyday realities of network defense.

To this end, we introduce the Offense Death Cycle (ODC), a CPT-aligned operational concept for defenders. Rather than a prescriptive framework, the ODC is best understood as a way of structuring defensive thinking around proactive environmental control. It translates the strategic logic of continuous interaction and contestable initiative into a practical method of proactive environmental control, where defenders:

(1) Bridge strategic theory and operational cyber defense by applying persistence as a method, not merely a condition to endure.
(2) Deliberately induce friction as a defensive tactic, exploiting the attacker's dependence on stable environmental conditions.
(3) Integrate reactive incident handling with continuous initiative management, creating a feedback loop that grows more effective over time.

2 THEORETICAL FOUNDATIONS

2.1 Persistent Interaction and Contestable Initiative

Cyber Persistence Theory (Fischerkeller, Goldman, and Harknett 2022) identifies cyberspace as a structurally interconnected environment defined by constant contact between actors. Because this contact is continuous rather than episodic, strategic advantage depends on maintaining initiative, not deterrence. Traditional deterrence theory assumes that credible threats of retaliation or denial can prevent adversaries from acting (Libicki 2009); CPT instead argues that in a domain of constant contact, there is no stable pre-attack state to preserve. Adversaries are already operating, and security depends on contesting their initiative rather than threatening consequences for action.

Security, therefore, rests on seizing and sustaining initiative. At the outset, attackers typically hold it: they choose the time, scope, and methods of their operations. Yet initiative is contestable: it can be seized, lost, and regained through successive operations. The central question for defense is thus not how to prevent or stop attacks, but how to act persistently to shape the conditions under which they unfold.

For the defender, the implication is profound. If initiative is not fixed but contestable, defense need not remain reactive. A defender who continuously shapes the environment—rather than waiting to respond—can (re)claim initiative. The ODC builds directly on this insight: it operationalizes the contest for initiative at the network level, treating every defensive action as a move in a persistent interaction rather than a response to a discrete event.

2.2 Offensive Cyber as Organized Bureaucracy

Network Attacks and Exploitation (Monte 2015) provides a useful operational lens for understanding modern offensive cyber campaigns. It describes them as complex organizational systems composed of interdependent phases such as targeting, initial access, persistence, expansion, and exfiltration. Each phase depends on the successful completion of previous ones and on stable conditions within the target environment.

Monte's taxonomy exposes both attacker and defender frictions – human, technical, and procedural constraints that shape the tempo and reliability of operations. Attackers must coordinate people, develop or acquire exploits, maintain tooling, establish infrastructure, and

manage bureaucratic processes. A failure or disruption in any one of these dependencies can cascade through the operation, imposing delays, costs, or outright mission failure. This organizational view matters because it converts abstract "threats" into observable, disruptible processes. Rather than facing an omniscient adversary, the defender faces a bureaucratic organization whose mission depends on specific conditions being met within the defended environment. The defender who understands these conditions can target them.

Smeets (2022) complements this view through the PETIO model (People, Exploits, Tools, Infrastructure, and Organization), which identifies the core components of offensive capability. Each element introduces specific dependencies on the environment: operators require stable access and familiar workflows, exploits depend on unpatched software, tools rely on stable configurations and predictable telemetry, infrastructure requires persistent network routes and service availability, and organizations depend on predictable schedules and reliable communication channels.

Together, these perspectives reveal that offensive cyber operations are not singular attacks but organizational processes with social and technical dependencies and flow in a constructed environment – cyberspace. The defender's insight is that each element is both an attacker's strength and a potential vulnerability: each dependency on environmental stability is a lever the defender can pull. Deliberate disruption of those processes – friction – can yield more than tactical gains: if the defender seizes the initiative through anticipation, the very environment that produces attackers' operational gains can be reconfigured so that offense becomes inefficient and costly. Treating the opponent not as an abstract "adversary" but as an assemblage of components allows the defender to deliberately control and shape the environment, thereby more holistically setting the stage for better defense than offense.

2.3 Asymmetries and Frictions in Cyber Operations

Monte's (2015) analysis identifies several persistent asymmetries – inherent advantages – and frictions between attack and defense. Attackers benefit from several clear asymmetries. Their motivation is high, driven by the high potential for gain with low risk of loss; failure teaches them quietly rather than exposing them publicly. They hold the starting initiative, while forcing defenders into reaction. Their focus is narrow and deliberate, in contrast to the defender's broad and divided attention. Generally, attackers possess deeper technical knowledge of targeted systems, craft precise, sometimes one-off, custom tools, and exploit the slower defensive rate of change.

Still, attackers face steady frictions. Mistakes expose them; complexity multiplies risks; flawed tools conflict and cause system outages. A single system update can erase access, while rival attackers can disrupt their operations. The security community shortens the life of exploits through vulnerability disclosure. Random chance – mis-timed commands, unexpected reboots, ad-hoc malware scans – adds uncertainty to every mission.

Defenders, meanwhile, have quiet but decisive asymmetries too. They possess total potential awareness of their networks and full control over their posture – able to reconfigure, segment, patch, replace, or temporarily shut down systems or networks at will. This defender's power to change the environment forces attackers to continually adapt and often invalidates their effort. However, exercising this power carries real costs: environmental changes disrupt users, consume IT staff time, and may conflict with operational requirements. The ODC does not ignore these costs; it proposes that they be weighed deliberately against the defensive value of friction generated, and that organizations start with low-disruption, high-friction actions before escalating.

Defensive frictions are also in play: human mistakes, flawed software, bureaucratic inertia, complexity, careless users, and plain bad luck. Yet when weighed together, the equation balances. Attackers may start with initiative, but defenders, owning the terrain and able to reshape it, hold the enduring home-field advantage. As Gleicher (2022) argued in a related context, the defender's structural advantage is precisely this ability to change the playing field. Per CPT, initiative is contestable: an attacker's starting initiative can be overturned by the defenders' ability to impose friction faster than the attacker can adapt (Fischerkeller, Goldman, and Harknett 2022). Thus, reaping the benefits of CPT requires defenders to turn asymmetry into an advantage through relentless environmental management.

2.4 From Theory to Operational Concept

The theoretical landscape reviewed provides three key building blocks:

(1) *CPT supplies the strategic logic*: cyberspace is a domain of persistent interaction where initiative determines security while being contestable through continuous action (Fischerkeller, Goldman, and Harknett 2022)
(2) *Monte (2015) supplies the operational anatomy*: offensive cyber campaigns are complex organizational processes with identifiable dependencies, phases, and frictions that make them vulnerable to disruption
(3) *The PETIO framework (Smeets 2022) supplies the capability model*: each element of offensive capability can be mapped to specific environmental conditions that the defender controls.

What none of these provides, individually or together, is a practitioner-applicable concept that translates strategic logic and operational insight into a repeatable method for enterprise defenders. The ODC is designed to fill this gap. It integrates CPT's strategic logic, Monte's operational anatomy, and Smeets's capability model into a coherent three-phase loop that enables enterprise defenders to act persistently within their own domain, imposing cumulative costs on attackers while generating increasingly refined intelligence.

3 THE OFFENSE DEATH CYCLE

3.1 Concept Overview

The Offense Death Cycle (ODC) is a continuous three-phase loop through which defenders apply and leverage proactive environmental control (Figure 1).

Each phase builds upon the previous one, forming a feedback system that replaces the linear *detect–respond–remediate–recover* logic with perpetual initiative management. The three-phase structure is intentionally simple and operationally driven. Intelligence establishes what to target, friction generates the defensive effect, and anticipation harvests the results and feeds the next cycle. Additional phases could be imagined, but splitting the loop further would add complexity without operational benefit; conversely, collapsing it into fewer phases would lose the crucial distinction between preparation, deliberate action, and systematic observation of its effects.

The loop is designed to be compatible with existing SOC workflows. It does not replace detection and response; it layers a proactive cycle on top of them. Organizations already performing threat intelligence, change management, and threat hunting possess the capabilities needed to operate an ODC; the framework provides the logic that connects these activities into a coherent offensive-against-offense posture.

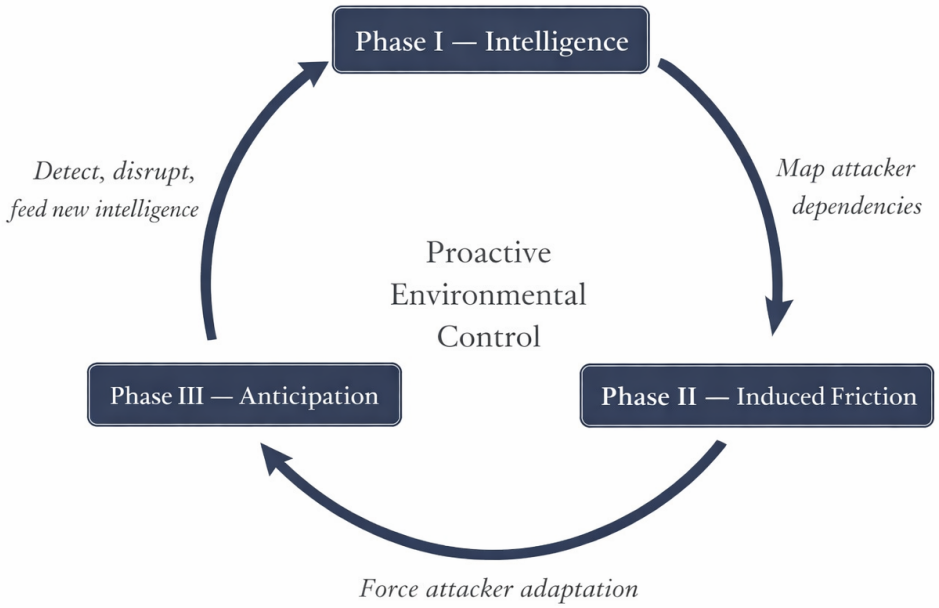

Figure 1. The Offense Death Cycle (ODC)

3.2 Phase I – Intelligence

Defenders begin by conducting reverse reconnaissance: analysing attacker TTPs not as discrete behaviors but as manifestations of their capabilities, requirements, and vulnerabilities (CRV).

Where conventional threat intelligence asks "what is the attacker doing?", the ODC's intelligence phase asks "what does the attacker need from our environment?". This CRV analysis draws on the PETIO model (Smeets 2022) to identify what the attacker requires across each dimension: stable credentials (People), unpatched software (Exploits), predictable configurations (Tools), persistent network routes (Infrastructure), and regular schedules (Organization). It draws on Monte's (2015) operational anatomy to understand how these dependencies interact across the phases of an offensive campaign.

The output of this *Intelligence* phase is a map of attacker dependencies within the defender's own systems and networks. This map is not static; it evolves with each cycle as new intelligence is gathered from the *Anticipation* phase. Over successive iterations, the map becomes increasingly refined, enabling more precisely targeted friction.

3.3 Phase II – Induced Friction

Once dependencies are understood, defenders apply friction by changing the environment on which those dependencies rely. These changes may be genuine – sudden system-wide credential rotation, unscheduled network segmentation, unannounced software upgrades, shifts in telemetry-generating activities; or fabricated – simulated oversight events, negotiated security services procurement, or red-team exercises masquerading as a rival APT.

The selection of friction mechanisms is guided by the CRV-PETIO mapping (see Section 4.1) and by the organizational constraints of the defending environment. Not all friction is equally costly to the defender or equally disruptive to the attacker; the goal is to maximize the cost ratio of attacker adaptation to defender implementation. Low-disruption, high-friction actions – such as credential rotation, telemetry shifts, and simulated audits – should typically precede more operationally disruptive measures. This graduated approach addresses the legitimate concern that environmental changes impose costs on the organization's own users and IT operations.

Each imposed change forces the attacker into adaptation, consuming resources and increasing detectable activity. Conducted within the defender's own administrative domain, such actions are legally sanctioned and operationally contained. This is a crucial distinction from Active Cyber Defense or deception approaches: the ODC's friction mechanisms are, individually, ordinary and genuine administration activities. Their defensive power comes from their deliberate selection, timing, and cumulative application.

3.4 Phase III – Anticipation

As attackers adapt to the induced friction – shifting TTPs, repairing access, or altering infrastructure – defenders monitor for signs of adaptation. These movements often expose previously hidden access points or reveal new attacker methods, tools, and infrastructure. The anticipation phase is where the ODC most clearly diverges from both Moving Target Defense (MTD) (which does not systematically observe the effects of its changes) and conventional detection (which looks for known indicators rather than adaptive behavior).

By detecting and removing these findings, defenders disrupt the attackers' persistence and feed new intelligence into the next cycle. This phase completes the loop: observation leads back to understanding, and the cycle repeats with increasing efficiency. With each iteration, the defender's CRV map becomes more detailed, the friction mechanisms become more precisely targeted, and the attacker's adaptation costs escalate. Over time, the attacker's campaign economics deteriorate: each cycle of re-tooling, re-entry, and re-establishing persistence costs more than the last, while the defender's cycle becomes more efficient through accumulated intelligence.

4 OPERATIONALIZING THE OFFENSE DEATH CYCLE

4.1 CRV–PETIO mapping

Because attackers and defenders operate in the same environment, every attacker's capability and supporting requirement creates a potential lever of friction available to the defender. Building on the PETIO model (Smeets 2022), Table 1 shows tactical examples of this capability-to-friction mapping.

Table 1. CRV–PETIO Mapping: Attacker Dependencies and Defender Control Levers

Capability	Attacker Requirement	Defender Control Lever vs Attacker Vulnerability
People	Consistent operator access, credentials, behavior patterns	Rotate privileges and passwords, enforce MFA, shorten session lifetimes, shift telemetry
Exploits	Stable, unpatched software builds	Apply unpredictable patching and version upgrades
Tools	Dependence on host fingerprints, telemetry stability, configurations, rule exceptions	Alter telemetry and logging patterns, normalize configurations, review or reset rules to secure default
Infrastructure	Fixed network routes, persistent jump hosts, external services usage patterns	Re-segment networks, change DNS, introduce ephemeral hosts, temporarily shutdown systems, shape traffic
Organization	Predictable change schedules, change announcements, observable communications, known response patterns	Unannounced upgrades, simulated audits, irregular maintenance windows, red-on-red simulation

This mapping serves as a guide for friction selection in the initial ODC cycle and as a starting point for more deliberate and creative friction synthesis in subsequent iterations. Defenders should treat the table as illustrative rather than exhaustive: operational environments differ, and the most effective friction mechanisms will be those tailored to the specific attacker profile and defended infrastructure.

4.2 Operational Vignettes

The following operational vignettes draw on the author's direct experience and anonymized practitioner engagements. They are presented as illustrative examples of how ODC interventions can be enacted in practice, rather than as formal incident reports. These vignettes should be read as operational patterns and control concepts, not prescriptive playbooks.

Trigger Overwatch. Simulate imminent external oversight – for example, the announcement of a new managed security services provider engagement or a deep third-party IT security audit. In this case, the intelligence phase identified that the attacker tended to intensify operations prior to periods of heightened organizational attention, suggesting a higher discovery risk tolerance in the face of losing access. The fabricated oversight event forced the attacker to attempt broadening persistent access, increasing operational tempo to implement rushed reconfiguration, which increased error rates and detectable activity. These observable adaptations then fed the anticipation phase, revealing previously hidden access vectors.

Simulate Red-on-Red. Introduce controlled artifacts resembling rival APT activity. CRV analysis indicated that the attacker monitored for competitor presence within the target environment. The induced friction from perceived competition provoked premature or noisy actions, significantly increasing detection likelihood. The anticipation phase harvested the attacker's reactive movements, yielding new intelligence about their tooling and persistence mechanisms.

Sudden Change Management. Execute unannounced reconfigurations, emergency patching, or unscheduled software upgrades within controlled parameters. These environmental changes broke the attacker's persistent access and automated exfiltration routines, forcing re-entry attempts that surfaced previously hidden access. Monitoring for these re-entry attempts constituted the anticipation phase.

Bad Luck Injection. Introduce benign, contained instability: short periods of downtime or controlled restarts; intermittent bandwidth throttling; randomized rescheduling of administrative and security tasks. This targets the attacker's reliance on predictable operational rhythms. The effect disrupted attacker automation and timing, increased manual interventions, and raised operational costs and error rates.

Each of these measures reflects a legitimate system-administration action repurposed for operational effect. Individually trivial, their cumulative application degrades attacker confidence and operational efficiency. *Operational Note:* Any deliberate environmental change – scheduled or unscheduled – requires prior risk assessment, formal change-management approval, rollback plans, and legal or ethical review. Organizations should align ODC interventions with their incident-handling, change-control, and compliance frameworks to avoid unintended service outages or regulatory exposure (NIST 2018; ISO/IEC 2022).

4.3 Illustrative Cases

The following cases draw on well-documented, high-profile incidents and illustrate how environmental change repeatedly emerges as a decisive variable in real-world defensive operations. They highlight the mechanism – *environmental change → friction → attacker exposure or failure* – even where such changes were not designed as deliberate ODC interventions. The cases are organized into two categories: *accidental friction*, where unintended environmental changes disrupted ongoing intrusions, and *deliberate environmental control*, where proactive choices about infrastructure and architecture pre-empted the success of attacks.

Accidental Friction: Visibility Transitions. Many high-profile APT detections exhibit a common pattern: the introduction of new or enhanced defensive mechanisms exposes operations already in progress. These are not typical cases of detection through static defenses but *visibility-transition detections* where an environmental change forces adversary exposure. The ODC framework interprets these as frictions – instances where the defender's reconfiguration disrupted the attacker's adaptation equilibrium and made persistence untenable.

Equifax (2017). Attackers exploited a known Apache Struts vulnerability (CVE-2017-5638) in mid-May 2017 and maintained undetected persistence within Equifax's dispute-resolution web application for over two months. During this period, encrypted outbound traffic concealed continuous data exfiltration, while Equifax's network monitoring remained ineffective: the SSL inspection certificate on a core sensor had expired in November 2016, preventing decryption of outbound traffic (U.S. GAO 2018). On 29 July 2017, an administrator renewed the expired certificate – a routine maintenance action with no defensive intent. This administrative reset restored decryption and immediately altered the operational environment. The attacker's workflow depended on a stable, opaque telemetry state; once that opacity lifted, the command-and-control traffic became visible. Within hours, the monitoring system generated alerts on anomalous outbound connections, prompting containment actions the next day (U.S. GAO 2018; U.S. House of Representatives 2018).

From the ODC perspective, Equifax shows that even unintentional resets of the defensive environment can trigger the cycle's terminal phase. The certificate renewal reconfigured the terrain, broke the attacker's adaptation equilibrium, and exposed their persistence. Discovery was a product of restored environmental control – a case where the defender's benign action imposed friction severe enough to terminate an ongoing operation. The ODC's argument is that this effect, produced accidentally at Equifax, can be produced deliberately and repeatedly.

Marriott/Starwood (2018). Starwood's reservation network had been compromised since 2014. The breach surfaced in late 2018 after Marriott's internal monitoring tools, introduced during post-acquisition integration, flagged the attacker's persistent access. Detection stemmed

from an environmental change – new telemetry and system integration – not from routine detection and incident response (Marriott International 2018; U.S. SEC 2019).

DNC (2016) and OPM (2015). Similar dynamics are visible in both cases: the decisive factor was a transition in visibility brought about by the introduction of new security tooling. At the DNC, CrowdStrike's Falcon EDR suite, deployed in May 2016, immediately identified live command-and-control traffic from two threat groups (CrowdStrike 2016). At OPM, newly deployed commercial detection software revealed beaconing activity disguised as a legitimate McAfee component (U.S. House of Representatives 2015, 2016). In each case, the new defensive mechanism altered the operational environment and inadvertently disrupted the conditions under which the attacker had achieved stable persistence.

These cases do not represent deliberate ODC operations. They illustrate the mechanism: an environmental change – even an accidental one – can impose friction that breaks an attacker's persistence equilibrium. The ODC proposes making this mechanism deliberate, continuous, and intelligence-driven.

Deliberate Environmental Control: PrivatBank (2017). In June 2017, the NotPetya wiper worm swept through Ukraine's public and private sectors, crippling government, logistics, banking, and industrial networks. Yet PrivatBank, the country's largest financial institution, remained largely unaffected. Its resilience was not incidental; it stemmed from long-standing environmental choices exemplifying the principles of proactive environmental control.

Years before the attack, PrivatBank had migrated its internal infrastructure to Linux years earlier, announcing in 2013 that it had become "the world's largest corporate user of Linux" (PrivatBank 2013). By 2017, its core banking environment operated on a proprietary platform, *PrivatLinux*, isolated from user-facing and administrative networks through strict segmentation (PrivatBank 2017a). When NotPetya propagated through interconnected Windows domains using credential reuse and SMB vulnerabilities, these barriers – rooted in incompatible authentication models and minimal trust relationships – stopped the worm's operational chain – discovery, propagation, privilege escalation, and destruction – at each boundary. Contemporaneous reports confirmed that PrivatBank's electronic services "were not subjected to hacker attacks" and continued operating normally during the outbreak (PrivatBank 2017b).

From the ODC perspective, this immunity reflects proactive environmental control as a deliberate defensive instrument. The defender neither detected nor blocked the attack, but had pre-shaped the environment so that the adversary's automation – dependent on predictable and homogeneous conditions – failed to adapt. The heterogeneous operating environment and enforced segmentation acted as designed frictions – each domain boundary forced the attacker to restart its campaign logic from zero. PrivatBank thus illustrates deliberate ODC in practice: a defender using long-term proactive environmental control to impose friction, deny persistence, and render a large-scale offensive operation self-terminating.

5 POSITIONING THE OFFENSE DEATH CYCLE WITHIN CYBER DEFENSE APPROACHES

The idea that defenders should move beyond reactive postures is not new. Over the past decade, a range of research programs, doctrinal frameworks, and practitioner-oriented models have explored how defenders might act more proactively in cyberspace. This section surveys the most relevant approaches, clarifies where the ODC aligns or diverges, and highlights the specific gap it is intended to address.

Table 2 summarizes how the ODC relates to existing approaches. As illustrated, the ODC occupies a specific niche: it is the only approach that combines real environmental shaping with an intelligence feedback loop, in a form designed for enterprise practitioners. It does not claim to supersede any of the approaches; rather, it integrates insights from Moving Target Defense (environmental change as a weapon), Active Cyber Defense (initiative over reaction), deception (exploitation of attacker expectations), and Cyber Persistence Theory (persistent interaction as the defining condition of cyberspace) into a single operational loop.

5.1 Moving Target Defense (MTD)

The Moving Target Defense (MTD) program, initiated under U.S. Army Research Office sponsorship, proposed that defenders can create asymmetric uncertainty by dynamically changing system configurations, IP addresses, software variants, and network topologies (Jajodia et al. 2011). MTD rests on a simple but powerful premise: static systems are inherently advantageous to attackers. If the target remains stable, the attacker can accumulate knowledge and refine their operations accordingly. By introducing continuous variation at the technical level—through mechanisms such as address-space randomization, software diversity, or network resegmentation— MTD forces attackers to operate against a shifting target rather than a fixed one.

The ODC shares this core intuition: environmental change disadvantages the attacker. However, it departs from MTD in both scope and logic. MTD is primarily technical and often automated, focusing on parameter randomization to increase uncertainty. It is algorithmically driven and does not explicitly incorporate an intelligence feedback loop linking defensive actions to observed attacker behavior. The ODC operates at a broader operational level. It treats MTD-style technical changes as only one category of friction among others, alongside procedural, organizational, and even deceptive/cognitive measures. Most importantly, the ODC's three-phase loop connects friction generation to intelligence about attacker dependencies and anticipation of attacker adaptation, creating a cumulative cycle rather than a set of randomization techniques. The result is not simply variability, but a cumulative process of shaping attacker behavior over time.

5.2 Active Cyber Defense (ACD)

Active Cyber Defense (ACD) broadened the defensive vocabulary beyond firewalls and signature-based detection. Denning (2014) articulated a framework inspired by active air and missile defense, encompassing a spectrum from internal defensive measures to external countermeasures. Her framework admits a wide range of actions, from threat intelligence and honeypots to strike-back operations, and articulates six ethical and legal principles governing their use. Herring and Willett (2014), writing from within the NSA's Information Assurance Directorate, offered a complementary vision of real-time cyber defense integrating threat sensing, sense-making, and decision-making into a continuous operational loop.

The ODC follows the ACD tradition's rejection of purely reactive defense and its emphasis on initiative. Where it diverges is in scope and mechanism. ACD literature encompasses actions both within and beyond the defender's network boundary, including offensive countermeasures that raise legal and operational concerns. The ODC is deliberately constrained to the defender's own administrative domain – it achieves its effects through shaping the defended environment rather than through actions directed at the attacker's infrastructure. This makes the ODC legally uncomplicated and operationally self-contained: every action it prescribes is a legitimate administration measure. Furthermore, while ACD tends to focus on real-time responses to observed threats, the ODC centres on proactive environmental shaping that operates continuously, independent of if or when a specific threat has been detected.

5.3 Cyber Deception and Counter-Exploitation

A substantial body of work has examined how defenders can influence attacker behavior through deception. Deception is situational and relies on environmental additions – decoy assets, honeytokens, and segmented traps – designed to lure or observe an attacker in controlled spaces (Pawlick, Colbert, and Zhu 2019; MITRE 2021). Its effectiveness depends on whether the attacker becomes aware of, interacts with, or is influenced by these synthetic elements. More sophisticated approaches to cyber deception, such as those articulated by Heckman et al. (2015) and Bodmer et al. (2012) propose multi-layered deception campaigns integrated with intelligence analysis, and counter-exploitation operations that apply counter-intelligence tradecraft to digital environments. Complementing these approaches, Pawlick, Colbert, and Zhu (2019) provided a game-theoretic taxonomy, showing how defenders can optimize deceptive strategies under various assumptions about attacker rationality. These approaches share the ODC's view of the attacker as an organized entity.

The ODC acknowledges the value of deception and can incorporate deceptive measures as one mechanism of friction generation – for example, through fabricated oversight events or artifacts resembling rival APT activity. However, the ODC does not depend on the attacker engaging with synthetic elements. Instead, it treats the entire defended environment as dynamic terrain – subject to deliberate change by the defender to induce operational friction.

Its fundamental mechanism is the alteration of the real operational environment. Where deception introduces artificial constructs to trap or mislead, the ODC modifies actual conditions: system configurations, credentials, network topologies, and operational tempo. The distinction matters because sophisticated attackers may detect and discard synthetic elements, but they cannot ignore genuine environmental changes that complicate or invalidate their established access and tooling. The ODC and deception are thus complementary: deception enriches the friction palette (fabricated artifacts, false signals, counter-exploitation traps), while the ODC provides the operational loop within which deceptive and genuine environmental changes are planned, executed, and assessed for effect.

5.4 Game-theoretic Approaches

Game theory has been applied to cyber defense to formalize the strategic interaction between attacker and defender as a mathematical contest. Subrahmanian et al. (2016) developed game-theoretic models integrating deception with proactive defense, analyzing equilibrium strategies and payoff structures for adversarial interactions in networks. These models provide analytical tools for understanding when and how defenders should act, and under what conditions proactive strategies dominate reactive ones.

The ODC operates at a different level of abstraction. Where game-theoretic models require formalized utility functions, payoff matrices, and equilibrium analysis, the ODC provides a practitioner-applicable operational loop. The two approaches are complementary: game-theoretic analysis could inform friction-selection decisions within an ODC cycle – for example, by modeling which environmental changes impose the greatest adaptation costs on a given attacker profile. Future research integrating game-theoretic optimization with the ODC's operational structure could yield significant advances for both fields.

5.5 Resilience Models

Resilience-oriented approaches focus on the defender's ability to absorb, adapt to, and recover from disruption. The E.U. DYNAMO project developed a resilience cycle comprising six phases – Prepare, Prevent, Protect, Detect, Respond, Recover – that emphasizes continuous coordination and threat intelligence exchange across critical infrastructure sectors (Rajamäki et al. 2018).

Resilience models share with the ODC a cyclical structure and a commitment to continuous operation rather than one-time incident response. Yet, their orientation differs fundamentally. Resilience is recovery-centric: it assumes that attacks will succeed and seeks to minimize impact and restore function. The ODC centers on imposing costs and seizing initiative: it treats intrusion not as failure requiring recovery but as interaction requiring management. Where resilience asks "how do we bounce back?", the ODC asks "how do we make the attacker's persistence untenable?". The ODC can operate alongside resilience frameworks, with resilience providing the recovery baseline and the ODC providing the proactive initiative layer.

5.6 Military Doctrine

U.S. Joint Publication 3-12, Cyberspace Operations (JCS 2023), provides the doctrinal framework for U.S. military cyber operations. It defines Defensive Cyberspace Operations (DCO) and distinguishes between internal defensive measures (DCO-IDM) and response actions (DCO-RA), including activities to detect, characterize, counter, and mitigate threats within defended networks. JP 3-12's framing of cyberspace as an operational domain structured around manoeuvre, fires, and protection resonates with ODC's emphasis on environmental control.

Beyond U.S. doctrine, the United Kingdom's National Cyber Force articulated a complementary operational philosophy in *Responsible Cyber Power in Practice* (National Cyber Force 2023). The document frames cyber operations in terms of shaping adversary behavior by exploiting their reliance on digital technology, and argues that "the greatest cognitive effect" is often achieved "by affecting the functionality and effectiveness of an adversary's systems over a period of time" rather than through outright denial – a "bend-but-do-not-break approach." As Fischerkeller, Harknett, and Goldman (2023) note, this approach closely reflects the logic of CPT, in which actors continuously set and reset conditions of their own security. The emphasis on cumulative campaign effects and gradual erosion of adversary confidence resonates directly with ODC's concept of induced friction and cumulative cost imposition.

The ODC translates this doctrinal intent into a form applicable outside military command structures. JP 3-12 is designed for joint force commanders and presupposes military authorities, intelligence support, and operational chains of command. Enterprise security teams, critical infrastructure operators, and national CERTs operate under different constraints and authorities. The ODC provides a bridge: it applies the strategic logic of persistent engagement and environmental control to the civilian and enterprise contexts, using organizational and administrative levers rather than military ones.

5.7 Defensive Mechanisms: from Predictable Obstacles to Intentional Friction

Existing defensive mechanisms, such as firewalls, anti-malware tools, or SIEM systems, typically function as predictable features of the defender's environment. They predate an offensive operation, can be discovered through reconnaissance, bypassed through planning, or neutralized through operational means. By contrast, frictions do not exist as fixed artifacts. They emerge unpredictably from the interaction between the attacker's expectations and the defender's deliberate actions. Defensive mechanisms introduced later in an operation may generate friction when they unexpectedly collide with the attacker's workflow – breaking dependencies the attacker relied on. In such cases, the mechanism itself is not the friction; rather, the friction is the unforeseen increase in observability and control of the environment that results from its introduction. The illustrative cases (Section 4.3) demonstrate this dynamic.

Table 2. Positioning the Offense Death Cycle (ODC) Among Cyber Defense Approaches

Approach	Core premise	Environment shaping	Intelligence feedback loop	Practitioner applicability	Key limitations
Cyber Kill Chain	Model attack as linear phases to enable disruption	No	Limited (post-detection)	High (detection-focused)	Linear; reactive
ATT&CK / D3FEND	Structure attacker behavior and defensive mappings	No	No	High (analysis and mapping)	Descriptive; no interaction model
Moving Target Defense	Introduce variability to increase attacker uncertainty	Yes (technical, automated)	No	Moderate (algorithmic)	No strategic feedback loop; narrow scope
Active Cyber Defense	Enable proactive and real-time defensive action	Partial (context-dependent)	Partial	Variable	Legal complexity; unclear operational boundaries
Cyber Deception	Influence attacker behavior through synthetic artifacts	Yes (synthetic environment)	Partial (via interaction)	Moderate	Depends on attacker engagement
Game Theory	Model attacker–defender interaction analytically	Conceptual (via strategy)	Conceptual (equilibrium-based)	Low (analytical)	Not directly operationalizable
Resilience (DYNAMO)	Ensure continuity through absorption and recovery	Indirect	Yes (adaptive cycle)	Moderate	Recovery-oriented; does not seek initiative
JP 3-12 DCO	Military doctrine for defensive cyber operations	Yes (operational domain)	Yes	Limited (military context)	Not directly applicable to enterprise environments
ODC	Proactively shape environment to impose friction and contest initiative	Yes (real environment)	Yes (3-phase loop)	High (enterprise SOC)	Conceptual stage; requires empirical validation

6 IMPLEMENTATION AND EVALUATION

6.1 Toward Evaluation Metrics

Assessing the effectiveness of proactive environmental control is inherently more challenging than measuring reactive detection and response. This section offers preliminary ideas for how organizations might begin to operationalize ODC assessment, acknowledging that rigorous empirical validation remains a task for future research. At a conceptual level, ODC performance can be approached through two complementary classes of indicators: defender-driven inputs and attacker-observable effects.

Friction inputs capture the defender's deliberate environmental interventions – the frequency, scope, and diversity of changes introduced into the system. These mirror standard cybersecurity process metrics but are assessed through their disruptive rather than preventive or detective value.

Attacker reactions capture detectable changes in attacker behavior following these interventions. These may include re-exploitation attempts, C2 rotation, shortened dwell time, or increased visibility of adaptive behavior. In this sense, these extend conventional detection metrics by treating the attacker's adaptive activity as a measure of friction achieved. In practice, however, measuring attacker reactions is difficult. Distinguishing re-exploitation by the same actor from independent scanning by unrelated attackers requires strong attribution capabilities. Observing C2 rotation presupposes that initial C2 channels are being monitored rather than simply blocked. Many adaptive behaviors may occur partially or entirely outside the defender's visibility. These challenges do not invalidate the concept, but underscore that ODC metrics must be interpreted cautiously and within context.

Ratio of time-to-adapt vs. time-to-reset. The principal ODC performance concept is the comparison of defender reset cycles to attacker adaptation cycles. When the defender's cycle outpaces the attacker's, persistence becomes economically and operationally unsustainable. An alternative metric – *effort-to-adapt* vs. *effort-to-reset* – may prove more practical in specific operational contexts but is more demanding in terms of observation capability, threat intelligence, and behavioral analysis. These ratios can be tracked alongside standard SOC benchmarks – mean time to detect (MTTD) and mean time to respond (MTTR) (Chiarini et al. 2023). Instead of measuring reaction to compromise, however, they quantify the defender's ability to impose continual change and thereby deny long-term stability to the attacker.

6.2 Organizational Considerations

SOC transformation. Implementing the ODC entails a fundamental shift in the SOC's mission, from monitoring and reacting toward proactive environmental management. Its mandate must expand beyond telemetry collection and analysis to include the authority and capability to initiate, plan, supervise, and directly introduce deliberate environmental changes.

IT–security Coordination. In many organizations, IT operations and cybersecurity are separate functions with distinct reporting lines, priorities, and incentive structures. The ODC inherently requires both: security teams to identify friction opportunities through CRV analysis, while IT operations possess the access and expertise to implement environmental changes. This organizational split presents a real challenge. Possible coordination models include: embedded security engineers within IT operations teams; joint change-advisory boards with authority to approve ODC interventions; or the proposed Cyber Defense Operator role, described below, as a bridge between security intelligence and IT implementation. Regardless of model, senior leadership must grant the SOC explicit authority to initiate environmental changes for defensive purposes – a significant governance shift that requires sustained executive support.

Roles. With this shift, SOC personnel require broader operational permissions and closer integration with system administration and change management processes (ISO/IEC 2023; NIST 2018). Several existing roles must be extended:

- Threat analyst – expands from TTP-oriented analysis to conduct CRV research and map attacker dependencies. This role investigates not only tools and techniques, but also attackers' organizational structures, behavioral patterns, standard operating procedures, and operational trends.
- SOC analyst – extends traditional detection and response functions to include the observation of attacker adaptation. This involves tracking the effects of induced friction and correlating defensive interventions with measurable changes in adversary behavior.
- SOC manager – acts as an organizational catalyst, translating intent into action by coordinating stakeholders, negotiating authority, and driving the bureaucratic processes required to implement timely and repeatable environmental changes.

In addition, a new role is introduced:

- Cyber defense operator – responsible for executing controlled environmental changes and fabricating or deploying deceptive artifacts. This role bridges the gap between security intelligence and IT implementation, requiring both deep technical knowledge of the defended environment and an understanding of attacker operational patterns.

Cost management. Environmental changes impose real costs on users and IT staff. Unscheduled credential rotations can frustrate users; unannounced reconfigurations may disrupt services; irregular maintenance windows can strain IT resources. The ODC does not treat these costs as negligible. Rather, it proposes that organizations weigh them deliberately against the defensive value of the friction generated. A graduated approach is therefore recommended. Organizations should begin with low-disruption, high-friction interventions (e.g., credential rotation, telemetry shifts, or simulated audits) before escalating to more operationally disruptive measures (e.g., network re-segmentation or unscheduled system upgrades). Over time, as

the organization accumulates experience with ODC operations, the cost–benefit assessment can be refined and calibrated to the organization's risk tolerance and operational constraints.

In parallel, strengthened governance and safety mechanisms are necessary to ensure that all environmental interventions remain operationally sound, risk-contained, and aligned with broader organizational policy (ISO/IEC 27001:2022).

7 STRATEGIC AND OPERATIONAL IMPLICATIONS

7.1 Strategic Implications

The ODC reframes cyber defense as persistent, proactive environmental control rather than a sequence of detection, reaction, and response. By continuously shaping terrain, defenders transform home-field advantage (Gleicher 2022) into an instrument of initiative. In CPT terms, they act persistently to set the conditions of security, converting a reactive posture into an ongoing campaign for initiative.

Strategically, this approach restores agency to the defender. Instead of seeking deterrence by denial (i.e., convincing adversaries that attacks cannot succeed and therefore should not be attempted), ODC achieves operational exhaustion through cost imposition: forcing attackers into repeated adaptation cycles that drain capability, tempo, confidence, and morale. While deterrence by denial relies on adversary perception and rational calculation before an operation, ODC operates during ongoing intrusions, degrading campaigns already underway. Over time, the defender's capacity to impose friction and reset conditions faster than the attacker can adapt becomes a self-reinforcing strategic advantage.

Unlike resilience models, ODC does not treat intrusions as failures but as interactions to be managed. This normalization of constant contact undercuts the attacker's dominance, introducing persistence, initiative, and control as the conceptual basis of cyber defense. Where resilience asks *how to recover*, and active defense asks *how to counter*, ODC asks *how to make the attacker's environment untenable*. This represents a distinct strategic posture—one that complements existing approaches while re-centering initiative as the defining condition of cyber defense.

7.2 Operational Implications

At the operational level, the ODC provides a bridge between strategic concepts such as persistence and the daily practices of SOC operations. It complements MITRE's ATT&CK and D3FEND frameworks by focusing on the attacker–defender interaction within a shared, contested environment rather than on taxonomies of attacker capabilities (MITRE, n.d.; Kaloroumakis et al. 2021). Rather than organizing work primarily around analysis, detection, and response, the ODC encourages defenders to design, implement, and assess deliberate environmental changes as part of routine operations. This shift has practical consequences for how defensive

work is structured and experienced. Teams are no longer limited to reacting to alerts, but can actively influence adversary behavior and operational conditions. While morale is ultimately a strategic asset, it emerges here as an operational effect: teams that can act decisively and shape outcomes tend to sustain higher levels of engagement and initiative than those confined to reactive workflows.

7.3 Research and Future Work

The ODC is presented as a conceptual framework; empirical validation remains an important next step. Future research should examine how induced friction affects attacker efficiency, adaptability, and campaign durability.

Several avenues are promising. Agent-based simulations could model attacker decision cycles under varying levels of environmental change, helping defenders to identify effective friction strategies. Game-theoretic modeling, building on Subrahmanian et al. (2016) and Pawlick, Colbert, and Zhu (2019), could formalize intervention strategies and identify optimal intervention timing.

Empirical studies are equally important. Structured case study research, including analysis of real-world defensive operations, could provide evidence of how ODC principles manifest in practice (something our illustrative cases gesture toward). Red team exercises specifically designed to test ODC operations – particularly those measuring attacker adaptation costs – would yield particularly valuable insights.

Finally, the integration of ODC with existing capabilities warrants further exploration. Integrating ODC with deception platforms and threat intelligence systems may further amplify its effects. In particular, the relationship between environmental control and deception—both grounded in attacker dependence on environmental conditions—offers a promising direction for developing more effective, integrated defensive approaches.

8 CONCLUSION

The Offense Death Cycle (ODC) operationalizes Cyber Persistence Theory for cyber defense: in a domain of constant contact, security arises not from reaction but from deliberate action (Fischerkeller, Goldman, and Harknett 2022). It reframes defense from a sequence of detection, response, and remediation into a continuous practice of environmental control. By leveraging friction as a tactic and home-field advantage as an operational asset, defenders can contest initiative and impose cumulative cost on persistent attackers.

For SOC leaders and defense planners, the ODC challenges a foundational assumption: that the defender's role is to detect and respond to attacker actions. Instead, it positions defense as the active shaping of conditions under which those actions occur. In this view, success is not defined by interrupting individual attacks, but by making them progressively more costly,

more visible, and ultimately unsustainable. While elements of this logic appear in Moving Target Defense, Active Cyber Defense, deception research, and military doctrine, the ODC brings these strands together into a single, practitioner-oriented operational loop grounded in the logic of persistence.

The ODC is deliberately presented as a starting point rather than a finished model. It invites practitioners to test, adapt, and refine it within their own operational environments, and calls for empirical research to assess its effectiveness and limitations. The author hopes this framework proves useful—not because it offers all the answers, but because it reframes the question: not "*how do we stop the attacker?*" but "*how do we make the attacker's job impossible?*"

ABOUT THE AUTHOR

Volodymyr Styran is a Special Assistant to the Chairman of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) and a co-founder of Berezha Security Group with OSCP, CISSP, and CISA credentials. He specializes in techniques, frameworks, and strategy of cyber conflicts. He co-founded NoNameCon conference and OWASP Kyiv chapter, co-hosts the No Name Podcast. In 2022, he joined Ukraine's cyber defense forces in response to the russia's full-scale invasion.

ACKNOWLEDGMENTS

The author thanks Michael Fischerkeller, Emily Goldman, and Richard Harknett for their generous and formative engagement with the ODC concept—including talking the author out of grounding it in sabotage theory, which in hindsight was proactive environmental control applied to the manuscript itself; and the editors and anonymous reviewers who provided feedback that was, in the best spirit of the ODC, both disruptive and improving.

REFERENCES

Bodmer, Sean, Max Kilger, Gregory Carpenter, and Jade Jones. 2012. *Reverse Deception: Organized Cyber Threat Counter-Exploitation.* New York: McGraw-Hill.

Chiarini, Francesco, Désirée Sacher-Boldewin, Logan Wilkins, and Mark Zajicek. 2023. *Security Incident Timing Metrics (SITM), Version 1.0.* FIRST.Org, Inc., May 29, 2023. https://www.first.org/global/sigs/metrics/Security-Incident-Timing-Metrics_v1.0.pdf.

CrowdStrike. 2016. "Bears in the Midst: Intrusion into the Democratic National Committee," June 4, 2016. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

Denning, Dorothy E. 2014. "Framework and Principles for Active Cyber Defense." *Computers & Security* 40:108–113. https://doi.org/10.1016/j.cose.2013.11.004.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace.* Oxford: Oxford University Press.

Fischerkeller, Michael P., Richard J. Harknett, and Emily O. Goldman. 2023. "UK NCF, Responsible Cyber Power, and Cyber Persistence Theory," April 5, 2023. https://www.lawfaremedia.org/article/uk-national-cyber-force-responsible-cyber-power-and-cyber-persistence-theory.

U.S. GAO (U.S. Government Accountability Office). 2018. *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach.* GAO-18-559. Washington, DC, August 30, 2018. https://www.gao.gov/products/gao-18-559.

Gleicher, Nathaniel. 2022. *Keynote Address, International Conference on Cyber Conflict (CyCon'22).* Tallinn, Estonia. https://www.youtube.com/watch?v=ULQ4RZedRlQ.

Heckman, Kristin E., Frank J. Stech, Ben S. Schmoker, and Roshan K. Thomas. 2015. *Cyber Denial, Deception and Counter Strategies.* Cham: Springer.

Herring, Michael J., and Keith D. Willett. 2014. "Active Cyber Defense: A Vision for Real-Time Cyber Defense." *Journal of Information Warfare* 13 (2): 46–55.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. 2011. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* Lockheed Martin. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

ISO/IEC. 2022. *Information Security Management Systems — Requirements (ISO/IEC 27001:2022).* Geneva. https://www.iso.org/standard/27001.

ISO/IEC. 2023. *Information Security Incident Management — Part 1 (ISO/IEC 27035-1:2023).* Geneva. https://www.iso.org/standard/78973.html.

Jajodia, Sushil, Anup K. Ghosh, Vipin Swarup, Cliff Wang, and X. Sean Wang, eds. 2011. *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats.* New York: Springer.

JCS (Joint Chiefs of Staff). 2023. *Cyberspace Operations (Joint Publication 3-12).* Washington, DC.

Kaloroumakis, Peter E., et al. 2021. *Toward a Knowledge Graph of Cybersecurity Countermeasures.* MITRE. https://d3fend.mitre.org/resources/D3FEND.pdf.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Marriott International. 2018. "Marriott Announces Starwood Guest Reservation Database Security Incident," November 30, 2018. https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident.

MITRE. 2021. "Active Defense: Using Deception and Trickery to Defeat Cyber Adversaries." https://www.mitre.org/news-insights/impact-story/active-defense-using-deception-and-trickery-defeat-cyber-adversaries.

MITRE. n.d. "MITRE ATT&CK: Adversary Tactics and Techniques." https://attack.mitre.org.

Monte, Matthew. 2015. *Network Attacks and Exploitation: A Framework.* Indianapolis: Wiley.

National Cyber Force. 2023. *Responsible Cyber Power in Practice.* Gov.UK, April 4, 2023. https://www.gov.uk/government/publications/responsible-cyber-power-in-practice.

NIST (National Institute of Standards and Technology). 2018. *Computer Security Incident Handling Guide (SP 800-61 Rev. 2).* Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-61r2.

Pawlick, Jeffrey, Edward Colbert, and Quanyan Zhu. 2019. "A Game-Theoretic Taxonomy and Survey of Defensive Deception." *ACM Computing Surveys* 52 (4). https://doi.org/10.1145/3337772.

PrivatBank. 2013. "PrivatBank Has Become the World's Largest Corporate User of Linux," September 26, 2013.

PrivatBank. 2017a. "PrivatBank and its Electronic Services Were Not Subjected to Hacker Attacks," June 27, 2017. https://privatbank.ua/news/2017/6/27/privatbank-i-yogo-elektronni-servisi-ne-piddavalisya-atakam-hakeriv-pres-sluzhba-banku.

PrivatBank. 2017b. "PrivatBank Proposed Secure Corporate Systems Based on PrivatLinux," June 30, 2017. https://privatbank.ua/news/2017/6/30/privatbank-zaproponuvav-derzhavi-bezpechni-korporativni-sistemi-na-bazi-privatlinux.

Rajamäki, Jyri, et al. 2018. "Cyber Threat Intelligence Exchange for Critical Infrastructure." In *Proceedings of the European Conference on Cyber Warfare and Security (ECCWS).* Academic Conferences International.

U.S. SEC (U.S. Securities and Exchange Commission). 2019. *Form 8-K: Disclosure of Starwood Guest Reservation Database Security Incident.* https://www.sec.gov/Archives/edgar/data/1048286/000162828018014745/a2018ex99.htm.

Smeets, Max. 2022. *No Shortcuts: Why States Struggle to Develop a Military Cyber Force.* New York and London: Hurst Publishers / Oxford University Press.

Subrahmanian, V. S., et al. 2016. *Game Theory for Cyber Deception and Defense: Final Report.* AD1055617. DARPA.

U.S. House of Representatives. 2015. *OPM Data Breach Hearing.* Washington, DC, June 16, 2015. https://www.govinfo.gov/content/pkg/CHRG-114hhrg99659/pdf/CHRG-114hhrg99659.pdf.

U.S. House of Representatives. 2016. *OPM Data Breach: Part II.* Washington, DC, July 12, 2016. https://www.govinfo.gov/content/pkg/CHRG-114hhrg22363/html/CHRG-114hhrg22363.htm.

U.S. House of Representatives. 2018. *The Equifax Data Breach.* Washington, DC. https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

Received 27 October 2025; Revised 20 March 2026; Accepted 25 March 2026