Military Cyber Affairs

Volume 6
Issue 1 *HammerCon 2023 Issue*

Article 4

May 2023

Operationalizing Deterrence by Denial in the Cyber Domain

Gentry Lane

Operationalizing Deterrence by Denial in the Cyber Domain

Gentry Lane

Introduction

For more than a decade, the major threat actors (Russia, China, Iran, and North Korea) and others have invested considerable resources to stand up and develop military cyber commands. Their offensive operations vary in tactics, techniques and procedures (TTP), have a broad range of targets, variable mission success rates, and they deploy offensive cyber operations (OCO) during times of peace, strategic competition and wartime. Brazen and pernicious, the sheer scale and persistence of state-sponsored malicious cyber activity is unprecedented. No other operational domain, especially during times outside of war, has been a vector for comparable persistent belligerence.

Despite the tacit threat of retribution from the world's most lethal military and largest nuclear power, adversary OCO on domestic American targets persists. Furthermore, iterative improvements in TTP suggest that adversary cyber forces are learning from mistakes and committed to improvement. Since rational actors discontinue unsuccessful campaigns, the accelerating scale, scope and sophistication of OCO implies satisfaction with mission success levels and an intention to continue the current escalating trajectory.

While successful offensive cyber campaigns outcomes lack the body count, permanence or physical damage of kinetic attacks, decades-long aggression on the seemingly inviolable American homeland is a remarkable achievement that should not be devalued. Despite an absence of visible destruction, the result is nonetheless impactful. When examined individually, low and medium-impact cyber events are inconsequential to the nation's security posture. However, the cumulative effect of sustained, incremental, repetitive erosion of critical assets and institutions poses an existential threat to the Western way of life. Temporary disruptions to critical services are inconvenient, but a campaign that gradually produces a nation-wide loss of trust in the integrity of critical infrastructure is pernicious.

In lieu of a cohesive counteroffensive strategy, the U.S. counters cyber aggression with small teams of forward-deployed operators, crisis triage and reactionary lines of effort from a myriad of loosely coordinated stakeholders. This approach yields stopgap solutions, piecemeal strategy and, notably, continued mission success for adversaries. This myopic response and lack of a viable, cohesive counteroffensive does nothing to deter adversary operations, and in fact perpetuates an unvirtuous cycle of exploitation, that draws the U.S. further into a quagmire of resource and power attrition.

The current triage-focused, reactive counteroffensive strategy is and will always be inadequate because the scope and scale of advanced persistent threat (APT)-perpetuated aggression is beyond the security capacity of any one nation. The ever-expanding attack surface is too big, the adversaries are too numerous, and the pace of battle is too fast. Hardening every critical target to the point of impenetrability is impossible. Even carefully constructed layered security stacks will be rife with software, supply chain or insider threat vulnerabilities. An iron dome-protected or Balkanized sovereign splinternet defeats the purpose of a free, open, interoperable internet as envisioned.

Worse, the U.S.'s current security posture is predicated on denying a hypothetical catastrophic "cyber Pearl Harbor" attack. Preparation for a catastrophic attack is at odds with the major threat actors' salami slicing tactics to incrementally cause harm while staying below the threshold of armed conflict. An alignment of adversary objective and counteroffensive strategy is an essential condition of victory. Misalignment usually guarantees defeat.

On Deterrence

The 2019 National Defense Authorization Act expressly calls for deterrence by stating "it shall be the policy of the United States, with respect to matters pertaining to cyberspace, cybersecurity and cyber warfare, that the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities."

The very complicated concept of strategic deterrence is frequently (and wrongly) reduced down to its most base elements: Imposing costs and establishing a credible threat of retaliation. While deterrence strategy certainly contains those elements, deterrence isn't achieved by simply establishing red lines or issuing sanctions. Despite a preponderance of PhD theses and articles proposing otherwise, there are only two types of deterrence and they fall under the strategic concept of *coercion*. Coercion is a strategy that leverages bargaining power created by threat of pain from punishment or a costly failure. Viable coercion strategies structure and align incentives to so that the adversary behaves in a desired way prompted either by force or by choice. Coercion can be divided into two types: *Compellence* and *deterrence*. Both strategies are for use after a conflict has started in order to bring about conflict resolution.

Compellence requires a significant direct action or credible threat of action that compels the adversary to behave in a desired way. The atomic and hydrogen bombs that ended World War II (WWII) were fundamental components of a viable compellence strategy. The U.S. compelled unconditional surrender at risk of nation-wide annihilation for Japan. Compellence is provocative, urgent, visible, and brutal by design.

The other subset of coercion is *deterrence*: *Deterrence by punishment* and *deterrence by denial*. Both forms are de-escalatory by nature because they are collaborative and afford the adversary agency.

Deterrence by punishment employs a credible threat of strong punishment in order to deter the adversary from taking an unwanted action. Deterrence by denial reduces the perceived benefits that an action is expected to provide to the aggressor. Simply put deterrence by punishment deters through fear of pain and deterrence by denial deters through fear of failure.

Deterrence by denial deters unwanted aggression by rendering adversary offensive operations impossible or unlikely to succeed, thus negatively impacting the adversary's cost-benefit calculus and prompting prioritization of other opportunities with higher likelihoods of success. Deterrence by denial occurs by manipulating conditions so that the enemy inevitably tries and fails, or the success occurs at such a cost (as in a Pyrrhic victory) or at such an inconsequential scale, that campaign continuation isn't a viable option.

In the current condition, the U.S. is inextricably engaged in persistent cyber conflict with skilled adversaries. Protracted cyber conflict engagement yields no benefit to the U.S., and diplomatic efforts to convince the major threat actors to abandon or to curb cyber aggression thus far have not succeeded. Without a radical change in strategy, it is unlikely that the major threat actors will abandon offensive cyber activities.

Despite doctrine with the word "strategy" in the title issued by both the Department of Defense (DoD), and the White House Office of National Cyber Director, these publications fail to present a cohesive, sustainable, strategy to deter nation-state aggression. "Persistent engagement" and "defend forward," the two pillars of current cyber operations, are lines of effort which are unviable as stand-alone strategies. While both gambits yield intermittent efficacy in shaping adversary behavior, there are limits to their effectiveness: They both necessitate prolonged engagement in a resource-intensive battle for an outcome of precarious security.

If status quo is undesirable, a new desired end state must be defined. Assuming that the U.S. wishes to end conflict and maintain its position as global hegemon, I propose novel three-point desired end state:

1. The cyber domain is no longer a theater of active conflict.

2. The U.S. and allies are not confined to a persistent counteroffensive posture.

3. The imminent threat of kinetic escalation or catastrophic accident is removed.

Affirmatively, deterrence by denial could achieve these objectives. Kinetic countermeasures, cyber compellence, and cyber deterrence by punishment can be removed as viable counteroffensive strategies as they pose significant risk of escalation.

Furthermore, deterrence by denial is strategic principle currently active in all other warfighting domains. Anti-access zones are theoretical: There are no physical barriers to reliably deny access to U.S. sovereign land, sea or airspace. Yet in modern military history, only two adversaries have dared to attack the American homeland. This marked lack of domestic attacks is not due to lack of capability, (nor lack of desire, presumedly). Adversaries opt not to invade or attack the U.S. because they understand:

1. The operation would likely be pre-empted and denied by the formidable anti-air, anti-maritime and ground capabilities of the U.S. Armed Forces.

2. Even if pre-emptive efforts failed and the adversary did achieve partial or total mission success, the ability to attribute and respond in a swift and proportionate manner is assured, rendering consequences more painful than any benefit gained from the attack.

This is by definition deterrence by denial: Pre-emptively denial is highly probably thus rendering mission success unlikely, or possible at a prohibitively high cost. Because of this high cost and low payoff calculation, and high risk of a painful retribution, the adversary discontinues the campaign by their own volition.

Ironically, the sustained condition of deterrence by denial in other operational domains is what renders the cyber domain such an attractive attack vector. In the cyber domain, adversary OCO's are met with little resistance, the risk of detection is very low, the chance of achieving mission success is very high, and the latencies in attribution and response all work to the adversary's advantage.

This begs the question: What capabilities could be operationalized in the cyber domain to negatively impact the adversary's risk/reward and cost/benefit calculi, while reliably denying mission success at scale, would not lead to escalation, and would provide the adversary a face-saving 'out,' all in a warfighting domain that lacks boundaries, traditional visibility and the battle pace happens at the speed of light?

This conundrum is not without historical precedence. In between the World Wars technologist rose to the challenge of defending immobile critical targets from well-obfuscated, extremely fast-moving threats. For Allied forces, the Luftwaffe was a rapidly approaching, lethal threat that was obfuscated by cloud cover, dark of night or distance. Situational awareness of incoming airplanes, despite a lack of traditional visibility, was the highest priority, and RADAR technology was developed into a defensive weapon platform.

It should be noted that while RADAR provided attribution and time to mitigate the oncoming air threat, early RADAR systems did not directly deter or deny adversaries. The deterrent effect came into play when the weapon platform was further developed into a global interoperable system. Interoperability was key: it greatly increased the scale of situational awareness and facilitated instantaneous sharing of standardized intelligence.

Essential Capabilities for Cyber Deterrence by Denial

New warfighting domains require new capabilities and modification of tried-and-true strategies. Cyberspace with its unique features—an ephemeral, borderless, binary battlefield that traverses all other warfighting domains—is no exception. When modifying deterrence by denial strategy to suit the conditions and constraints of cyberspace, the key difference is "impenetrability."' On land, sea and air critical assets are well guarded. If an offensive effect reaches its target, deterrence has not occurred.

Impenetrability is neither practical nor achievable in the cyber domain. The attack surface in cyberspace is simply too big, too complex and too dynamic to adequately secure without impeding the free flow of information or compromising reasonable privacy. However, in cyberspace deterrence can occur even if the target's initial lines of defense are breached. The adversary's operation must be denied before mission success is achieved for cyber deterrence by denial to occur.

Figure 1 shows the MITRE ATT&CK framework divided and labeled in special operations terms. Thinking of cyber operations this way is useful because we can see that mission success in the cyber domain occurs in the latter half of the kill chain (MITRE ATT&CK 6-7). Deterrence in cyberspace is contingent not on preventing initial breach, but by reliably denying the operation at some point in the kill chain before mission success can be achieved.

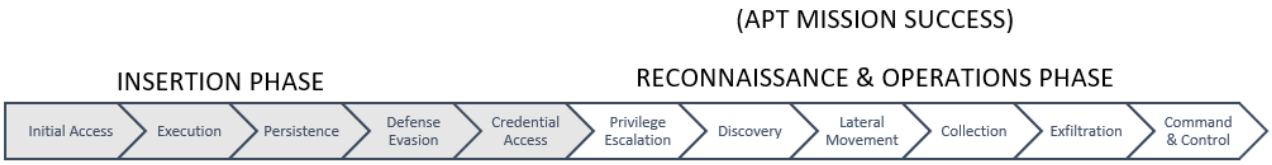

Figure 1. The MITRE ATT&CK Framework

Understanding the current technology gaps required to achieve an outcome of sustained deterrence is crucial. None of the commercial off-the-shelf or government-bespoke solutions in use today can reliably deny OCO mission success at scale. Timely situational awareness of APT activity in the civilian sector is currently unavailable to any security authority. The lack of traditional visibility and latency in determining conclusive attribution can and have been overcome in other

warfighting domains, but not in cyberspace. Given the level of technological sophistication at hand today (especially in the research labs that develop warfighting capabilities), few capability gaps are technically insurmountable. Yet technology and capability deficits persist. Without first understanding and acknowledging the nature of these capability gaps, resources for their realization will never be prioritized. Nor will these capabilities be valued or recognized as essential when they do appear.

To operationalize deterrence by denial in the cyber domain the following capabilities are required:

1. **A mechanism that permits visibility for early detection in order to negatively impact adversary cost/benefit calculus.**

RADAR and SONAR are spectrum-based visualization generators. They don't provide traditional visibility of a target, they provide a visual representations of a target's trajectory. Adversary cyber effects pass at light speed from host to host through a series of routers, transmitters and cables, as light pulses and radio signals among decillions of other signals. Because internet infrastructure can only facilitate linear delivery of packets of binary signals, the trajectory of a cyber effect is known, instantaneous and therefore irrelevant. Visibility becomes relevant when the offensive effect interacts with the target network, first traversing firewalls and/or deception software before reaching a target endpoint.

Fileless malware is a type of malicious code favored by sophisticated actors because it resides in endpoint memory, rendering it invisible and undetectable to all commercial solutions. Fileless malware (and other low observable characteristic tactics) allow adversaries to probe, map, build backdoors and execute the vast majority of reconnaissance work in memory without touching files where they can be detected. The only way to find adversary presence in memory is through a process called memory forensics.

Memory forensics is the industry standard security postmortem analysis because it is the deepest, most thorough analytic procedure. However, memory forensics is infrequently used because it requires a considerable amount of time and expertise to execute. (Typically, it takes one forensic expert two to three days to run memory forensics on one endpoint). Recent developments in the application of AI/ML automation have rapidly increased the speed, scale and accuracy of this process so that malicious behavior can be discovered and mitigated within the first four steps of the MITRE ATT&CK framework (without requiring a forensic expert).

Because OCO are weeks/months long incremental processes, finding evidence of adversary malicious behavior at the earliest stages of the kill chain (MITRE 1-5) allows for ample time for threat mitigation or further surveillance. If the vast majority of OCO are reliably discovered and denied before mission success can occur, the adversary's cost benefit calculus is negatively impacted.

2. **A mechanism for rapid attribution in order to negatively impact the adversary's risk calculus.**

Plausible deniability and the latency from time of detection to retribution are the key cyber domain-specific factors that work in the adversary's favor. Removing anonymity/plausible deniability and collapsing the delay from discovery to retribution would allow a rapid response which negatively impacts the adversary's risk calculus. Again, endpoint memory forensics is the current industry standard for security event attribution. By tracing and recreating the OCO progression through the MITRE ATT&CK framework, forensic analysis provides context to a security event which can support a theory of adversary intent. As mentioned earlier, recent developments in the application of AI/ML to automate this process increase the speed and scale of discovery, attribution and intention resolution from months to minutes.

3. **A computational mechanism that facilitates privacy-preserving federated analysis for anticipatory intelligence.**

By aggregating and inputting the totality of security event data over geographic, sector and time domains into predictive algorithms, important anticipatory intelligence could be gleaned. Because all military cyber forces are beholden to procedure and bureaucracy, they generate distinct behavioral patterns. These behavioral patterns, in context, can resolve both identity and intention. The ability to know –and rapidly share—analysis which indicates where, when, and how a major threat actor might strike next will further negatively impact both cost/benefit and risk calculi.

Understandably, nations and private-sector entities are reticent to share sensitive breach information. Advances in privacy-preserving cryptographic protocols (e.g., zero-knowledge encryption and secure-multiparty computation) permit multiple stakeholders the ability to analyze data and arrive at a mutually desired result without requiring parties of this transaction to divulge their private data.

A general rule for predictive analytics is that the more data yields lower estimation variance, ergo better predictions. The massive amounts of data generated by global APT behavior signatures in ultra high-fidelity binary analysis of endpoints around the globe is likely to reveal trends and behaviors that have previously been impossible to capture and of great value to defenders. To achieve statistically significant results, the data must be uniform and first party captured.

4. **The aforementioned capabilities integrated into a standardized, interoperable global platform that facilitates bilateral intelligence sharing at the speed of war, reserved exclusively for approved stakeholders.**

Because cyberspace is a borderless domain, lines of demarcation must be drawn along principle, not geographic position. Countries who agree to abide by an

unambiguous set of rules, norms and laws may obtain and sustain access to this global, interoperable early detection/rapid attribution defensive weapon platform. Only by democratizing these key capabilities and facilitating streamlined intelligence sharing among a coalition of allies, will a deterrent effect significant enough to shape adversary behavior occur.

Again, this situation is not without precedent. Society for Worldwide Interbank Financial Telecommunications, better known by its acronym SWIFT, is a financial industry communication platform that facilitates cross-border monetary transfers among a consortium of international stakeholders. This permission-based platform grants access only to a consortium of allied stakeholders who agree to abide by norms and laws. Revocation from the SWIFT network results in drastically slower, less secure and restricted financial transactions, thus incentivizing compliancy and punishing non-alliance members.

Standardization and global access to democratized capabilities also facilitates uniformity taxonomy (for reporting) and could enable standardization in retribution. Because the pace of battle happens at lightspeed in the cyber domain, the association between action and consequence weakens with time, for a punishment to be understood in its intended context, it must occur within minutes or hours of the trigger event.

Essential Conditions for Sustained Cyber Deterrence by Denial

Viable strategy is not a standalone determinator of battle success. Harmony between strategy, capability and condition is required. For a state of deterrence by denial to endure, the cyber theater must meet the following conditions:

1. An adversary that is committed to a grand national security strategy.

Long-term grand strategies are unique to nation-states. Terrorist organizations or criminal syndicates may have long-term objectives (e.g., cause harm to an enemy or enrich the organization), but they are not backed up by continuity of governance and state-sponsored armed forces require to realize grand strategies. Commitment to a grand strategy connotes an understanding of geopolitical rules/norms and that the actions have bearing and yield consequences in the global world order.

Therefore, deterrence by denial is not a viable strategy against anarchist or unstable regimes, nor for opportunistic adversaries (insider threats and ideology-driven terrorists), criminals or any for whom executing a long-term grand strategy is unrealistic, unavailable or irrelevant.

2. An adversary with a well-resourced, organized, offensive cyber force.

Adversaries who rely on a handful of ace hackers or hired proxies will not be deterred by repeatedly denied mission success because high talent turnover (or

off-prem proxies) provide a buffer between operators and commanders that artificially reduces the pain and impact of mission failure.

3. An objective understanding of adversary's values, fears and national will.

An unbiased, accurate assessment from the adversary's point-of-view is essential to craft compelling coercive elements and an enticing alignment of incentives. An inaccurate or hubris-influenced analysis will result in an ineffective, misaligned strategy. Likewise, an understanding of the limits of an adversary's complacency, the space where patience ends and the will to fight begins, must be identified in order to be avoided.

4. A reasonable understanding of an adversary's force capabilities at strategic, tactical and operational levels.

Accurate reconnaissance is vital to every battleplan. Counterintuitively, the establishment of robust offensive cyber forces does not guarantee operational efficacy and possession of cutting-edge capabilities is not a requisite for mission success. Even the most advanced actors prefer to use pre-existing exploits because they are more plentiful, familiar and easier to deploy.

5. Explicit interaction, entanglement and state of competition/conflict.

For deterrence to occur, the identities of all stakeholders must be explicitly clear, their retributive powers believable, and both parties must acknowledge (even if the acknowledgement is tacit) that they are engaged in competition/conflict. The major threat actors make regular use of proxies in an attempt to confound this dynamic, because deterrent threats have little effect on aggressors disassociated from state malicious actors. However, hired proxy groups are beholden to their nation-state sponsor as payment is usually commensurate with mission success.

6. The target(s) in question must be considered valuable by both parties.

Target(s) of temporary or inconsequential value do not justify the resources required to compose, implement and sustain major deterrence by denial operations for either aggressor or defender.

7. A mutual understanding that a sustained state of deterrence is contingent on the integrity of the defender and volition of the aggressor.

Even though the defender is the orchestrator of incentives and outcomes, both parties must believe that the aggressor is acting on their own volition. Equally important is continuous, irrefutable integrity in words and action by the defender. Any demonstrated unreliability by the defender will render an agreement, threat or redline moot.

The decision whether or not to engage rests in the aggressor's hands and the value in the collaborative aspect of deterrence by denial cannot be underestimated,

especially in multinational cyber conflict resolution. Affording the adversary agency to determine and decline engagement by their own volition is key to sustainability. Without adversary commitment, sustaining a long-term condition of deterrence is precarious. If an aggressor has no other choice but to engage, deterrence will not occur. Deterrence by denial is especially useful in conflicts with nations that are sensitive to great power inequities as it provides a face-saving alternative to acquiescence or surrender (which is key for sustaining the deterrence through administration changes and other geopolitical fluctuations).

8. Unambiguous, clearly communicated redlines.

Communicated through diplomatic, popular and military channels, the prohibited targets and placement of redlines must be presented in the simplest and least ambiguous terms so that understanding is irrefutable.

9. Unambiguous and time-sensitive threat of pain.

The aggressor must understand the defender's willingness and ability to use force:

(1.) In a timely manner,

(2.) Believe the intent to use this force is credible, and

(3.) Use of this force would result in significant detrimental impact.

Adversaries regularly exploit this latency as time delays soften hard blows. A security event will certainly seem less urgent and less relevant when discovered months or years after the fact. The latency between event and punishment is a factor that perpetuates both persistence and impunity.

Conclusion

The stakes are high. If state-sponsored cyber aggression is allowed to continue unchallenged, the United States risks losing its position of power…without being defeated in an armed conflict. The incremental, almost imperceptible erosion of stability in critical American assets, institutions and ability to project power is pernicious and effective. Opportunity, innovation, prosperity, free speech, and all the potential that the Internet brings are perpetually at risk when the cyber domain is an active theater of war. A viable counteroffensive strategy is urgently required.

A deterrence by denial strategy does not supplant other cyber (or national security) strategies. It is shortsighted at best, naïve at worst, to assume a multi-stakeholder conflict of this scale and complexity could be addressed by one overarching strategy or a few disparate lines of effort. American security relies on the condition of deterrence by denial in all other warfighting domains. The cyber domain should not be the exception.

The impunity which the major threat actors currently enjoy is not a permanent feature of the cyber domain. The current level of cyber domain aggression does not have to be the new normal, nor can it be without significant compromise to the modern way of life. Further cyber aggression must be deterred and reliably denied going forward (and the current damage reversed) if undoable damage is to be avoided.

About the Author

Gentry Lane a software architect, statistician and military strategy scholar. She is the CEO and Founder of ANOVA Intelligence, a cyber national security software company. Ms. Lane is a Senior Fellow at the Potomac Institute for Security Studies, a Fellow at the National Security Institute at George Mason University's Antonin Scalia Law School, a NATO STO technical panel member and on the academic paper review board.

References

2019 National Defense Authorization Act, 115th Congress, 2018.

Alex S. Wilner and Andreas Wegner (editors), *Deterrence by Denial from the Cold War to the 21st Century*, (New York: Cambria Press 2022), page 7.

Cory Bennett, "Obama urges China to stop cyber theft," The Hill, November 10, 2014.

Craig Timberg et al., "The Vulkan Files: Secret trove offers rare look into Russian cyberwar ambitions." The Washington Post, March 31, 2023.

Department of Defense Cyber Strategy (2018) https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

"Even the most advanced threats rely on unpatched systems," The Hacker News.com June 9, 2022

Gentry Lane, "Avoiding Cyber Forever Wars," NATO Joint Air Power Competence Center Conference Read Ahead, 2021, pg. 43

Gentry Lane, "Harnessing AI & Deep Learning for Real-Time Automated Advanced Persistent Threat Detection and Multi-Domain Situational Awareness," NATO Joint Air & Space Power Conference Read Ahead, 2020.

Louis Nelson, "Obama says he told Putin to 'cut it out' on Russian hacking," Politico, December 16, 2016.

Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military-Cyber Force*, (New York: Oxford University Press, 2022)

Matt Spetalnick, Michael Martina, "Obama announces 'understanding' with China's Xi on cyber theft, but remains wary," Reuters, September 25, 2015

McGhee, J. 2016. "Liberating Cyber Offense." Strategic Studies Quarterly 10/4 (Winter): 49

Michael P. Fishkeller, Emily O. Goldman, Richard Harknett, *Cyber Persistence Theory*, (New York, Oxford University Press, 2022).

"Persistent Engagement in Cyberspace is a Strategic Imperative," The National Interest, July 6, 2022.

Thomas C, Schelling, *Arms and Influence*, (New Haven: Yale University Press, 2008) pages 35-125.

White House National Security Strategy, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf