THE CYBER DEFENSE REVIEW
In press, 12 pages
https://doi.org/10.55682/cdr/5hkr-j1zh

SENIOR LEADER PERSPECTIVE

The Missing Grammar of Cyber Operations: Toward a Theory of Cyber Operational Art

LTG (Ret.) Edward Cardon[1], Dr. Charles Harry*[2]

[1]Army Cyber Institute, West Point, NY, USA
[2]University of Maryland, College Park, MD, USA

Cyber operations are now a permanent feature of modern conflict and competition, but they have not become a central component of modern war. Recent conflicts show that cyber can disrupt, degrade, deceive, and impose friction; yet, these effects rarely accumulate into sustained operational advantage. This essay argues that cyber lacks a mature operational grammar that allows commanders to arrange tactical actions in time, space, and purpose to achieve strategic objectives. Current doctrine is still relevant: it is the grammar used to implement that doctrine that differs for terrain, maneuver, fires, and effects, tempo, risk, and command. A separate theory of war or a new planning framework is not needed. What is needed is the understanding that the cyber terrain is socio-technical at its core, maneuver is positional, fires often consume access, tempo is governed by adaptation, risk accumulates over time, and command requires judgment across distributed authorities and consequences. The article advances a commander-centric framework for translating foundational concepts of military campaign design into the cyber domain.

Keywords: cyber operations, cyber warfare, operational art, cyber terrain, strategy

This essay introduces the foundational concepts of a broader theory of cyber operational art that is further developed in an upcoming book, entitled "Cyber Operational Art" (West Point Press, 2026).

* Corresponding author: charry@umd.edu

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*
© 2026 The Author(s) unless otherwise stated. As an open access journal, The Cyber Defense Review publishes articles under Creative Commons licenses, and authors retain copyright where applicable.

Lieutenant General (Retired) Ed Cardon serves as the United States Military Academy Academic Chair for Cyber. Over a distinguished 36-year military career, he has served in Germany, Bosnia-Herzegovina, Iraq, and the Republic of Korea. General Cardon has extensive experience establishing, leading, and transforming 14 organizations across a wide range of missions, including military operations, education, cybersecurity, and innovation. He commanded the 2d Infantry Division in the Republic of Korea and later transformed and scaled Army Cyber Command into a world-class cyber force. During that time, he also helped stand up several new cyber organizations to meet the demands of an increasingly contested domain, including U.S. Cyber Command's Task Force ARES, the offensive cyber task force targeting ISIS. Since retiring from government service, General Cardon has continued advising individuals, teams, and companies on complex challenges, drawing on deep expertise in operations, modernization, academia, cybersecurity, and national security.

Dr. Charles Harry is an Associate Research Professor at the University of Maryland's School of Public Policy and director of the Center for Governance of Technology and Systems (GoTech), where he leads research on cybersecurity, strategic risk, and the governance of complex technological systems. With more than 20 years of experience in intelligence and cyber operations, his work focuses on understanding and measuring the strategic effects of cyberattacks on critical infrastructure, organizations, and public systems. Prior to academia, Dr. Harry spent 14 years at the National Security Agency, where he led and supported complex cyber and intelligence operations in support of national security objectives, rising to senior technical leadership positions. He later led a major cybersecurity consulting organization serving both public and private sector clients. He has received multiple government and industry awards recognizing his leadership, operational contributions, and work advancing cybersecurity policy, research, and practice.

CYBER IS PRESENT BUT PERIPHERAL

For more than sixteen years, scholars, policymakers, and military leaders have debated whether cyberspace would transform warfare. Early arguments emphasized cyber's ability to strike across distance, bypass conventional defenses, disrupt critical infrastructure, obscure attribution, and impose costs below the threshold of armed conflict. Skeptics responded that cyber operations were more often instruments of espionage, sabotage, influence, or temporary disruption than decisive tools of war. The record of recent conflict has not resolved that debate.

Russia's 2022 invasion of Ukraine illustrates the problem. Russia entered the war with years of experience conducting cyber operations against Ukraine and a reputation as one of the world's most capable cyber powers. The opening phase included destructive cyber activity, including wiper attacks against Ukrainian government, information technology, energy, and financial organizations, as well as the Viasat KA-SAT attack that disrupted satellite broadband service on the first day of the invasion. Cyber operations mattered. They imposed friction, disrupted services, and supported broader Russian efforts to pressure the Ukrainian state. Yet they did not define the campaign. They did not collapse Ukrainian command and control, paralyze mobilization, challenge logistics, or remove the need for maneuver, fires, air defense, and territorial control. Cyber was present, but it was not campaign-organizing.

This pattern is not unique to Ukraine. Across contemporary competition and conflict, cyber operations are frequent, sophisticated, and consequential, but they rarely provide the organizing logic of military campaigns. States use cyber capabilities to steal, disrupt, degrade, deceive, prepare the environment, and impose costs. These activities can matter tactically and sometimes strategically. But they often appear as discrete actions appended to campaigns rather than as a means of designing campaigns. Cyber is everywhere in modern conflict, but it remains operationally peripheral.

Cyber has power because cyber operations can produce real effects. They can compromise networks, manipulate data, disrupt services, degrade processes, expose adversary activity, and impose friction on organizations. Nor is the answer simply that cyber is constrained by law, policy, or authorities, although those constraints matter. Operational art is the discipline that links tactical action to strategic purpose. In its most useful formulation, it is the arrangement of tactical actions in time, space, and purpose to achieve strategic aims. This definition matters because it shifts attention away from tools and toward employment. Military transformation does not occur simply because new capabilities exist. It occurs when commanders learn how to arrange those capabilities so that individual actions accumulate into operational advantage. Cyber has not made that transition. It has tools, accesses, malware, mission teams, doctrine, and authorities. What remains underdeveloped is a shared commander-centric language for explaining cyber terrain, how to maneuver on that terrain, when they should fire, how effects accumulate, how tempo is governed, and how risk is managed over time.

This missing grammar matters because tactical cyber success does not automatically become operational advantage. Access is not maneuver. Malware execution is not effect. Disruption is not necessarily leverage. A network map is not terrain. Speed is not tempo. Approval is not command. Risk is not merely a legal or policy obstacle; it is an operational variable that accumulates through access, presence, exposure, fires, adaptation, and escalation. Without a grammar for these concepts in the cyber domain, cyber operations remain difficult for commanders to integrate into campaign design. They can be requested, synchronized, and approved, but they rarely shape the campaign's central logic.

The argument advanced here is that cyber has become tactically capable and institutionally established, but it has not yet become reliably campaignable. Until this grammar is articulated, cyber will remain tactically impressive, strategically suggestive, and operationally incomplete. The task is not to prove that cyber is decisive in the abstract.

The task is to make cyber *campaignable*.

FROM CYBER WAR TO CYBER CAMPAIGNING

The scholarship on cyber conflict has moved through three broad phases. The first asked whether cyber would transform war. The second challenged that claim by emphasizing cyber's limits. The third, and most useful for military practitioners, has begun to shift the debates of cyber war to more nuanced discussions of campaigns. That transition matters because the central question is no longer whether cyber operations are "war," but how cyber operations can be arranged, sequenced, integrated, and assessed as part of military campaigns.

Early cyber scholarship and policy discourse often treated cyberspace as a potentially revolutionary strategic condition (Lynn III 2010). Cyber tools appeared to offer states a way to strike globally,

bypass conventional defenses, exploit civilian and military dependences on digital systems, obscure attribution, and impose costs below the threshold of armed conflict. In this view, cyber seemed to stretch inherited categories of war and peace. It promised strategic reach without traditional force projection, disruption without occupation, and coercion without the visible violence associated with conventional military power (Kello 2013). The appeal of this argument was clear: if modern societies and militaries depend on networked systems, then the ability to manipulate or disrupt those systems should create new forms of strategic leverage.

The skeptical literature corrected this early enthusiasm. Critics argued that cyber operations rarely perform the central functions historically associated with war (Rid 2012). They do not seize territory, destroy fielded forces at scale, compel surrender, or reliably produce durable coercive outcomes. Many cyber operations are better understood as espionage, sabotage, subversion, signaling, preparation of the environment, or temporary disruption (Gartzke 2013). This critique was necessary. It showed that technical access is not the same thing as strategic effect and that disruptive incidents should not be mistaken for military transformation. Cyber operations can impose costs and generate friction, but the empirical record has not supported the strongest claims that cyber would independently redefine war.

Yet the skeptical correction also created its own limitation. By focusing on what cyber has not achieved at the strategic level, it implied that cyber's military utility is inherently marginal. The fact that cyber operations rarely produce decisive strategic outcomes on their own does not mean they cannot matter operationally. The better question, therefore, is not whether cyber can replace conventional force. It is whether cyber can be employed in ways that create operational advantage when integrated with other forms of power (Libicki 2009).

This is where the literature has become more productive. A useful distinction separates strategic cyberwar from operational cyberwar (Libicki 2009). Using Libicki's construct, strategic cyberwar refers to cyber operations aimed directly at a state or society to alter behavior. Whereas operational cyberwar refers to cyber operations employed against military-relevant targets in the context of an ongoing or anticipated campaign. The first has often disappointed because cyber coercion is difficult to time, difficult to attribute clearly, difficult to repeat, and vulnerable to adaptation. The second is more promising because cyber effects need not be independently decisive to matter. They may delay mobilization, degrade command and control, disrupt logistics, corrupt data, impose uncertainty, expose adversary activity, or create windows of advantage for joint operations.

Recent work on cyber campaigns moves the field further in this direction by shifting the unit of analysis from isolated incidents to linked activity over time. Cyber operations are rarely best understood as single events. States often conduct connected sequences of reconnaissance, access development, exploitation, disruption, influence, and defense. These linked operations may unfold below the threshold of armed conflict, during crisis, or alongside conventional military operations (Harknett and Smeets 2022). Thinking in terms of campaigns helps explain how cyber activity can accumulate, shape an environment, and support broader strategic objectives.

But this turn toward cyber campaigns still leaves a missing layer. Campaigning requires an operational logic for deciding where to act, how to position, when to reveal or preserve access, what effects matter, how to pace activity, and how to manage risk. Without that logic, a series of cyber operations

may be connected administratively or temporally without becoming operationally coherent. Activity can accumulate without compounding outcomes.

The Russo-Ukrainian War makes this problem visible. Russia conducted cyber operations before and during the 2022 invasion, including destructive attacks and disruption of communications. Yet those operations did not reliably synchronize with maneuver, fires, logistics, or political objectives at campaign scale (Fischerkeller, Goldman, and Harknett 2026). Cyber activity was present, and at moments significant, but it did not become the organizing mechanism through which Russian military power achieved decisive advantage (Kostyuk and Gartzke 2022). The lesson is not that cyber is irrelevant. The lesson is that cyber effects are difficult to integrate without a mature grammar for terrain, maneuver, fires, tempo, risk, and command.

The field has therefore reached a useful but incomplete conclusion. The early debate over cyber war clarified the danger of technological determinism. The skeptical response clarified that cyber does not automatically produce strategic coercion. The campaign literature clarified that cyber operations must be studied as sequences rather than isolated events.

What remains underdeveloped is *cyber operational art*.

FROM TACTICAL EFFECTS TO OPERATIONAL GRAMMAR

Cyber's operational problem is not that cyber operations fail to produce effects. Cyber operations can compromise accounts, disrupt services, manipulate data, degrade systems, expose adversary activity, and impose friction across organizations. The problem is that these effects are often defined at the wrong level of analysis. A compromised account, disrupted service, encrypted server, or deployed payload may demonstrate technical success, but none of these necessarily answers the commander's basic question: *for what end?*

That question is unforgiving. Did the action delay mobilization, degrade command and control, impose decision friction, disrupt logistics, reduce confidence in data, or create a window of advantage for joint maneuver and joint fires? Did it change the adversary's behavior, capacity, coordination, or decision-making? Did it preserve friendly freedom of action or impose a dilemma the adversary had to resolve? If not, the cyber operation may have succeeded technically while failing operationally.

This distinction is central because cyber operations are often assessed through the language of technical activity. Access gained, malware deployed, credentials harvested, systems disrupted, data exfiltrated, and services denied are all meaningful to operators. None of this is sufficient for commanders. Operational art requires a different standard. Tactical actions matter only insofar as they accumulate into operational advantage and serve strategic purpose.

Cyber has a vocabulary of activity. It has tactics, techniques, and procedures; malware families; access concepts; mission categories; authorities; and doctrine. These are necessary. They allow cyber forces to plan and execute missions at a technical level. But they do not, by themselves, explain where cyber forces need to be positioned for a campaign, how cyber actions accumulate, when access should be preserved or expended, what counts as operational effect, how tempo should be governed, how risk changes over time, or how commanders should integrate cyber into campaign design.

The result is a recurring conceptual slippage. Access is treated as maneuver. Malware execution is treated as effect. Disruption is treated as leverage. Network maps are treated as terrain. Speed is treated as tempo. Approval is treated as command. Each error seems small, but together they explain why cyber remains operationally peripheral. Cyber actions may be synchronized with a campaign without shaping the campaign's logic. They may be approved without being commanded in an operational sense. They may create technical disruption without creating campaign advantage.

Terrain

Cyber operational art begins with terrain. In physical domains, terrain is often treated as something commanders discover, map, and exploit. Land forces assess ridgelines, rivers, roads, urban areas, and avenues of approach. Maritime forces consider chokepoints, littorals, sea lines of communication, and access. Air forces think in terms of altitude, range, basing, airspace, and sensor coverage. In each case, terrain provides the geometry of opportunity. It tells commanders where advantage may be created, where movement may be constrained, and where decisive action may occur.

Cyberspace does not provide terrain in this way. Its operationally relevant features are not self-evident. Servers, networks, accounts, cloud services, applications, databases, and control systems matter only because they enable human and organizational functions. A router is not key terrain simply because it is technically accessible. A server is not operationally important simply because it can be compromised. A network map is not terrain until it is linked to function.

Cyber terrain should be understood as a constructed *socio-technical system*. It is constructed by linking strategic functions to the organizational processes that sustain them, and then to the technical architectures through which those processes are enacted. Organizational processes includes users, permissions, data flows, dependencies, workarounds, vendors, and decision routines that allow an adversary to act.

Therefore, the commander's terrain question is not, "What network can we access?" It is, "What adversary function matters, what processes produce that function, and what technical systems and human dependencies sustain those processes?" If the objective is to delay mobilization, the relevant terrain may include personnel databases, transportation scheduling systems, fuel distribution processes, command approvals, logistics vendors, communications channels, and the users who maintain or bypass these systems. If the objective is to degrade air defense coordination, the relevant terrain may include sensors, command nodes, data links, operator procedures, identification protocols, and trust relationships between units.

This changes where cyber belongs in campaign design. Terrain construction is not merely technical reconnaissance or targeting preparation. It is an operational design activity, and this work also enables better cross-domain solutions. Until the terrain is constructed, commanders cannot know where cyber maneuver is possible, where fires might matter, what risks are worth accepting, or how effects should be assessed.

Maneuver

If terrain defines where advantage can be created, maneuver defines how forces position themselves to create options within that terrain. In traditional military theory, maneuver is the employment of forces

in time, space, and purpose to gain advantage over an adversary. The same logic applies in cyberspace, but the form changes because cyber maneuver is not simply access. Access is entry. Maneuver is the deliberate positioning of cyber capabilities across constructed terrain to create options, preserve freedom of action, and impose dilemmas. A force that gains access to one system has achieved a technical condition. A force that uses that access to understand dependencies, move laterally, establish redundant positions, preserve alternatives, and hold multiple adversary functions at risk has begun to maneuver.

This distinction matters because cyber operations often culminate when access is treated as the objective. Once access is gained, pressure builds to use it. But firing from the first available position may burn an opportunity without creating durable advantage. Maneuver asks whether access creates future choices, not merely whether it enables immediate action.

The commander's maneuver question is: "Does this position create options?" More specifically: Does it provide access to a function and process that matters? Does it reveal additional terrain? Does it create alternative avenues of approach? Does it preserve freedom of action if one access path is discovered or closed? Does it impose a dilemma on the adversary? Does it enable future fires at a time and place of the commander's choosing?

Cyber maneuver, therefore, includes access development, persistence, lateral movement, privilege escalation, defensive repositioning, deception, redundancy, and the shaping of adversary expectations. But those activities are operationally meaningful only when they expand the commander's choices across the constructed terrain. Access is preparation. Maneuver is the creation of operational options.

Fires and Effects

Fires are the point at which position becomes consequence. In cyberspace, fires are deliberate actions taken from positions of access to generate effects relevant to commander intent. They may disrupt, deny, degrade, deceive, manipulate, expose, or destroy. However, cyber fires differ from many fires in physical domains in one important respect: they often consume the very position that made cyber fires possible.

A cyber fire can reveal access, expose tools, trigger defensive learning, force credential resets, accelerate patching, or alert the adversary to a previously unknown vulnerability. The act of firing can convert permissive terrain into contested terrain. For that reason, cyber fires should be understood as expenditures of access. Cyber fires trade immediate effect for possible loss of future maneuver.

This is why the distinction between action, task, and effect is essential. *Actions* are what cyber forces do: phish users, exploit vulnerabilities, deploy malware, manipulate data, or generate traffic. *Tasks* are what systems experience: credentials are harvested, services degrade, files are encrypted, packets are dropped, or data is altered. *Effects* are what change in the adversary's ability to function: delayed decisions, reduced throughput, degraded coordination, mistrust of data, forced workarounds, or loss of confidence in a process.

The commander's fires question is not, "Can we execute the payload?" It is, "What functional change will this cyber (or other) fire produce, and is that change worth the access we may lose?" A denial-of-service attack against a public website may be visible and technically successful, but if the website is not tied to an operational function, the effect is trivial. Data manipulation inside a logistics system

may be less visible, but if it delays movement, corrupts confidence in scheduling, or forces manual verification during a critical phase, it may produce a meaningful operational effect.

Cyber effects must therefore be judged by functional consequence, not technical event. The effect is not what the system experiences: it is what changes in the adversary's behavior, capacity, coordination, or decision-making.

Tempo

Tempo in cyberspace is often mistaken for speed. Cyber operations occur in a domain where technical actions can move quickly, where vulnerabilities appear and disappear, and where defenders adapt rapidly. But speed is not tempo.

Cyber tempo is the pacing and sequencing of maneuver and fires relative to opportunity, exposure, and adversary adaptation. It governs when to act, when to wait, when to preserve access, when to reveal capability, when to impose pressure, and when to allow the adversary to move in ways that create future opportunities. Tempo is not the volume or rate of cyber activity but rather for cyber, tempo is the commander's control of adaptation.

This distinction is critical because cyber actions alter the terrain. Each action can generate indicators, expose methods, and provoke defensive response. Acting too quickly or too frequently can exhaust access and collapse future maneuver space. Acting too slowly can allow systems to harden, opportunities to close, or campaign windows to pass. Effective tempo requires judging the relationship between present effect and future option against adversary adaptation.

The commander's tempo question is: "Should we act now, wait, sequence this action with another effort, preserve access for a later phase, or force adaptation at a time of our choosing?" In some cases, the best cyber decision is restraint. In others, rapid action may be required before the adversary patches a vulnerability, shifts infrastructure, changes procedures, or begins a decisive operation. In other cases, cyber fires may be sequenced to coincide with physical maneuver, information operations, deception, or diplomatic pressure.

Tempo is what prevents cyber from becoming a series of isolated shots with limited or no effect. It links maneuver and fires across time and purpose. It allows commanders to preserve pressure without prematurely exhausting access. Without tempo, cyber activity becomes a collection of technical opportunities. With tempo, cyber operations can be paced to shape adversary adaptation and support campaign objectives.

Risk

Risk in cyber operations is often treated as an approval issue. The question centers around the question whether a proposed action is legally permissible, politically acceptable, technically feasible, or authorized at the proper level. Those questions matter. But they do not exhaust the operational meaning of risk.

Cyber risk is a cumulative tradeoff among mission gain, force exposure, access loss, escalation, assessment uncertainty, and future options. It accumulates through presence as well as action. Simply gaining access to a sensitive system may create risk to force, risk to sources and methods, risk of discovery, and risk to future maneuver. Firing from that position may add escalation risk, reveal

capability, or foreclose future use. Even restraint carries risk if it allows an adversary to adapt, move, or exploit an opportunity.

The commander's risk question is: "What do we gain now, what do we reveal, what options do we lose, and what adaptation or escalation do we trigger?" This question must be asked across the campaign, not only at the moment of execution. A technically limited action can generate significant operational consequences if it affects a sensitive process, becomes publicly visible, or forces political decision-making under uncertainty. Conversely, deep access in sensitive terrain may carry lower immediate escalation risk if no effect is produced, but higher risk to force if discovered.

Cyber risk therefore has several dimensions. There is *risk to mission*: the possibility that an action will fail to produce the intended functional effect or will undermine broader campaign objectives. There is *risk to force*: the possibility that tools, accesses, infrastructure, tradecraft, or intelligence equities will be exposed. There is *escalation risk*: the possibility that effects will trigger responses beyond what the commander intends. There is *assessment risk*: the possibility that technical indicators will be mistaken for operational consequence. And there is *opportunity risk*: the possibility that using an access now will prevent a more valuable use later.

A grammar of cyber operational art does not eliminate risk. It makes risk governable. It allows commanders to compare risks across time and purpose rather than treating them as isolated approval hurdles. This is essential because cyber risk is rarely static. It changes as terrain is discovered, maneuver expands, fires are employed, defenders adapt, and political conditions shift.

Command

Command is the element that converts grammar to action. Terrain, maneuver, fires, tempo, and risk do not combine automatically. In cyberspace, judgement is an important element because authority, access, effect, and consequence are often distributed across different organizations and levels of command.

Command should not be reduced to approval. Approval asks whether an action may occur. Command asks whether an action should occur, when it should occur, what purpose it serves, what risk it accepts, and what future options it preserves or sacrifices. Approval is a permission structure. Command is an operational judgment.

The commander's command question is: "Who owns the consequence of preserving or expending cyber position, and at what level should that decision be made?" Not every cyber action should be centralized. Excessive centralization can slow operations, eliminate initiative, and cause fleeting opportunities to disappear. But not every cyber action can be delegated. Some fires may create strategic consequences, expose sensitive capabilities, affect civilian systems, or alter escalation dynamics. The art of command is knowing which decisions can be pushed down and which must be retained.

This requires commanders to understand cyber effects in operational terms. They do not need to master every technical detail, but they must understand enough to judge terrain, position, effect, tempo, and risk. They must be able to ask whether a proposed action supports the campaign, whether it preserves or consumes future options, and whether the expected functional effect is worth the cost.

Command also includes restraint. In cyberspace, the decision not to fire can be as operationally significant as the decision to act. Preserving access may maintain leverage for a later phase. Maintaining ambiguity may reduce escalation pressure. Waiting may allow an adversary to reveal dependencies or create a more favorable window. Command is therefore not simply the authority to unleash cyber effects. It is the discipline to integrate cyber options into the campaign's broader logic.

Taken together, these six elements form the missing grammar of cyber operational art. Terrain defines where advantage can be created. Maneuver creates options across that terrain. Fires convert position into consequence. Tempo governs action against adaptation. Risk captures the costs of presence, exposure, and effect. Command integrates the whole through judgment. The purpose of this grammar is not to create a separate cyber theory of war. It is to make cyber legible within campaign design. Until commanders can reason in these terms, cyber operations will remain tactically capable but operationally incomplete.

MAKING CYBER CAMPAIGNABLE

Cyber operational art does not require a separate theory of war or a new planning system. The existing logic of joint campaign design already asks commanders to understand the operational environment, define the problem, develop an operational approach, arrange operations, assess effects, and manage risk. These are exactly the right questions. The problem is not that joint planning lacks space for cyber. The problem is that cyber often enters planning too late and in the wrong form.

When cyber is introduced late, it appears as an annex, a target nomination, an access request, or a discrete effect to be synchronized against a timeline already built around physical maneuver. Cyber participation is present, but is on the margins vice supporting the core plan. The result is familiar: cyber actions may be deconflicted, approved, and synchronized, but they do not necessarily create operational advantage.

The grammar developed above changes where cyber belongs in planning. Terrain, maneuver, fires, tempo, risk, and command are not cyber-specific add-ons. They are the concepts that make cyber intelligible for commanders and staffs within campaign design. They allow commanders and staffs to ask cyber questions at the same level of abstraction as other operational questions. The issue is not simply, "What cyber effects can support this plan?" The better question is, "How does the adversary's socio-technical terrain shape the problem, and what options can cyber create?"

This shift matters because campaigns are built around logic, not activity. A campaign is not a collection of actions placed on a timeline. It is an arrangement of actions in time, space, and purpose that changes conditions in ways that serve strategic objectives. If cyber operations are to become campaignable, they must be included in the design of that arrangement from the beginning.

This translation does not change the fundamentals of campaign design. This grammar makes cyber legible for campaign design. The operational environment is no longer understood only through geography, force disposition, and physical infrastructure. It also includes the socio-technical systems that produce adversary power. The problem is no longer framed only in terms of enemy forces, territory, or capabilities. It also includes the adversary functions that must be disrupted, delayed, degraded, defended, or manipulated to support the campaign.

Campaign design question	Cyber operational art translation
What is the operational environment?	What socio-technical terrain produces the adversary function we must affect or defend?
What is the problem?	Which adversary function must change, and why does that change matter to the campaign?
What is the operational approach?	How will cyber maneuver create options, preserve access, impose dilemmas, or enable joint action?
What are decisive points?	Which processes, identities, data flows, dependencies, or technical seams create disproportionate leverage?
How should actions be sequenced?	Which accesses should be preserved, which should be expended, and when?
What are fires?	Which cyber actions will generate functional effects, not merely technical events?
What is tempo?	How should cyber activity be paced against adversary adaptation and joint phasing?
What is risk?	What mission gain, force exposure, access loss, escalation risk, and future option cost accompany each action?
How is success assessed?	What changed in adversary behavior, capacity, coordination, decision-making, or process performance?
What must command decide?	Who owns the decision to preserve or expend cyber position, and at what level should that decision sit?

Table 1. Campaign Design Questions and their Translation into Cyber Operational Art

The practical implication is straightforward: cyber can shape the operational approach, not merely support one that has already been built. Late cyber integration asks, "What cyber effects can support this plan?" Early cyber integration asks, "What adversary functions matter, what terrain produces them, and what options can cyber create across that terrain?" The first question produces episodic support. The second begins to make cyber campaignable.

This does not mean cyber should dominate campaign design. In most conflicts, it will not. Physical maneuver, fires, logistics, alliances, political will, and territorial control will remain central to war. The purpose of cyber operational art is not to elevate cyber above other domains, but to allow commanders to use cyber coherently within the larger campaign. Cyber should be neither mystified as revolutionary nor dismissed as marginal. It should be judged by whether it creates options, imposes dilemmas, preserves freedom of action, and produces functional effects that matter.

CONCLUSION: AN UNGRAMMATICAL REVOLUTION

Cyber operations are not a failed revolution. They are an ungrammatical one. The tools exist, the forces exist, the authorities exist, and the effects are real. What remains underdeveloped is the operational language that allows commanders to turn cyber activity into campaign advantage.

The past sixteen years of debate have clarified what cyber is not. It is not a substitute for war. It does not reliably compel adversaries by itself. It does not remove the need for maneuver, fires, logistics, alliances, political judgment, or territorial control. But those limits do not make cyber irrelevant. They place cyber where most military capabilities belong: inside campaigns, where tactical actions must be arranged in time, space, and purpose to serve strategic aims.

To do this in the cyber domain, the right grammar is required. Commanders need to know what cyber terrain is, how cyber maneuver creates options, when cyber fires should be employed, how effects should be judged, how tempo should be paced against adaptation, how risk accumulates, and

who should own the decision to preserve or expend cyber position. Without that grammar, cyber will continue to appear in plans without shaping them. It will remain present but peripheral.

Cyber operational art does not require a separate theory of war. It requires translating familiar military concepts into a domain where terrain is constructed, maneuver is positional, fires often consume access, tempo is adaptive, and risk accumulates over time. If commanders can reason in those terms, cyber operations can become more than episodic disruption. They can create options, impose dilemmas, preserve freedom of action, and generate effects that accumulate toward strategic purpose.

Using the right grammar for operational art, cyber can deliver on its promise.

REFERENCES

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2026. "Why Alignment Matters: Cyber Capabilities and Military Operational Schemes in All-Domain Operations." *The Cyber Defense Review* 11 (1): 19–39. https://doi.org/10.55682/cdr/t41n-758s.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38 (2): 41–73. https://doi.org/10.1162/ISEC_a_00136.

Harknett, Richard J., and Max Smeets. 2022. "Cyber Campaigns and Strategic Outcomes." *Journal of Strategic Studies* 45 (4): 534–567. https://doi.org/10.1080/01402390.2021.1987095.

Kello, Lucas. 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38 (2): 7–40. https://doi.org/10.1162/ISEC_a_00138.

Kostyuk, Nadiya, and Erik Gartzke. 2022. "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine." *Texas National Security Review* 5 (3): 114–126. https://doi.org/10.26153/tsw/43733.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation. https://doi.org/10.7249/MG877.

Lynn III, William F. 2010. "Defending a New Domain—The Pentagon's Cyberstrategy." *Foreign Affairs* 89 (5): 97–108. https://www.jstor.org/stable/20788647.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5–32. https://doi.org/10.1080/01402390.2011.608939.