CYBER KEY TERRAIN: A CROSS-LEVEL RECONCILIATION FOR TACTICAL, OPERATIONAL, AND STRATEGIC CYBERSPACE OPERATIONS

Cezar VASILESCU[1]

Regional Department of Defense Resources Management Studies (DRESMARA) / „Carol I“ National Defense University, Brasov, Romania

The concept of cyber key terrain has emerged as a critical yet poorly defined element of military cyberspace operations. While the traditional military concept of key terrain translates well to the physical infrastructure of cyberspace, its application to virtual layers remains problematic. This paper identifies and analyses what we could call as the "cyber key terrain paradox": the concept demonstrates clear tactical utility when applied to physical network elements, but loses coherence and applicability at operational and strategic levels, where logical networks, cyber-persona dimensions, and cognitive layers become dominant. NATO's current promulgated doctrine, AJP-3.20 Edition A Version 1 (2020), adopts a three-layer model of cyberspace (physical, logical, and cyber-persona), while academic and doctrinal proposals have progressively expanded this to five, seven, and eight layers encompassing cognitive and social dimensions.

This proliferation of models intensifies rather than resolves the paradox, as no existing framework provides systematic terrain identification methodologies for the higher layers. Through systematic analysis of military doctrine and academic literature, this study reveals fundamental inconsistencies between narrow, physical-centric definitions of cyber key terrain and the broader, multi-layered character of cyberspace as a domain of conflict. The paper proposes a reconciliation framework comprising layer-specific adaptive definitions, a temporal classification system, and a structured identification methodology, preserving the concept's tactical utility while providing the doctrinal coherence that operational and strategic planning requires.

Key words: *cyber key terrain, cyberspace operations, military doctrine, cyberspace layers, operational levels.*

[1]ORCID ID: 0000-0002-5280-8795, e-mail: cvasilescu1@mapn.ro

1. INTRODUCTION

1.1. Cyberspace as the Fifth Military Domain

The recognition of cyberspace as the fifth military domain (alongside land, sea, air, and space) represents a fundamental shift in how modern militaries conceptualize conflict. This designation acknowledges that military operations increasingly depend on, occur within, and can be decisively influenced by activities in cyberspace. Unlike traditional physical domains defined by fixed geographic coordinates and tangible geography, cyberspace is simultaneously *physical* (hardware, cables, and electromagnetic signals) and *virtual* (software, data, protocols, personas); it is human-constructed however operates according to technical rather than natural laws; and it changes at speeds unprecedented in military history.

NATO's promulgated doctrine on cyberspace operations, AJP-3.20 Edition A Version 1 (NATO Standardization Office 2020), defines cyberspace as *"The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data"* (para. 1.13). The publication adopts a three-layer model (physical, logical, and cyber-persona) (paras. 1.9-1.12), and situates cyberspace operations within a broader Information Environment (IE) that *"comprises the information itself, the individuals, organizations and systems that receive, process and convey the information, as well as the cognitive, virtual and physical space in which this occurs"* (para. 1.3). This IE formulation implicitly acknowledges dimensions beyond the three-layer cyberspace model, including cognitive and social spaces, but does not integrate them into the formal domain structure. Meanwhile, academic and doctrinal proposals have progressively expanded cyberspace models:

- five planes encompassing geographic and supervisory layers (Raymond et al. 2014);
- five planes adding cognitive and socio-organizational dimensions (Grant 2014); and
- eight-layer model (geographic, physical, infrastructure, syntactic, semantic, services, persona, plus a mission layer) that explicitly incorporates human elements and geographic context and is the most comprehensive update to date (Venables 2021).

These expanded models underscore the multi-dimensional character of the space in which military operations must increasingly be planned and conducted.

1.2. The Cyber Key Terrain Paradox

This paper identifies the concept of *"cyber key terrain paradox"*: the concept of cyber key terrain demonstrates clear utility and relatively consistent application at tactical levels when focused on physical network infrastructure, however it becomes increasingly ambiguous, contested, and potentially inapplicable at operational and strategic levels where virtual and cognitive dimensions of cyberspace become dominant.

The management of physical cyberspace infrastructure as critical infrastructure presents distinct challenges that require specialized competencies and frameworks, as the physical layer forms the foundation upon which all other cyberspace operations depend (Codreanu 2020).

AJP-3.20(NATO Standardization Office 2020) does not define cyber key terrain as a formal term. The closest NATO doctrinal treatment remains the traditional key terrain definition from JP 2-01.3: *"Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant"* (Joint Chiefs of Staff 2009). Academic literature has adapted this concept to cyberspace: cyber terrain is defined as encompassing systems, devices, protocols, data, software, processes, cyber personas, and other networked entities (Raymond et al. 2014) or cyber key terrain defined as *"physical and logical elements of the domain that enable mission essential warfighting functions"*. (Bodeau et al. 2013)

The absence of a formal NATO-agreed cyber key terrain definition in AJP-3.20 is itself significant: it suggests that the Alliance has not yet resolved how to translate terrain concepts into the multi-dimensional cyberspace domain, a gap that becomes more acute as expanded layer models gain attention.

At the tactical level, identifying cyber key terrain appears manageable: critical routers, network nodes, servers, and communications links can be mapped, prioritized, and defended. At strategic levels, however, this clarity disappear. AJP-3.20's three-layer model already introduces challenges at the cyber-persona layer, where virtual identities lack the physical properties that terrain concepts assume (para. 1.12). When academic models expand the domain to include cognitive, social, and semantic layers, the terrain concept loses further coherence.

If strategic operations occur across multiple layers, but key terrain is defined mainly for the physical and lower virtual dimensions, how can the concept relate with strategic planning? This inconsistency represents the ***main research question*** this paper addresses.

1.3. Research Objectives

The research is guided by three interconnected **Research Objectives (RObj)**, as follows:

- **$RObj_1$** - systematically document the cyber key terrain paradox through analysis of military doctrine, including NATO's promulgated AJP-3.20, expanded academic cyberspace models and academic literature;
- **$RObj_2$** - analyze the sources and implications of definitional inconsistencies across tactical, operational, and strategic levels;
- **$RObj_3$** - evaluate whether the concept of key terrain can be meaningfully extended to the virtual and cognitive layers of cyberspace; and
- **$RObj_4$** - propose a reconciliation framework that preserves tactical utility while addressing operational and strategic requirements.

The hypothesis guiding the study is that the paradox is structural (the result of applying physical terrain concepts to a multi-dimensional domain) and that expanded cyberspace models proposed in academic literature make the paradox more rather than less acute, a problem compounded by the absence of terrain identification frameworks in NATO's current promulgated doctrine.

2. METHODOLOGY

The study employs a qualitative doctrinal analysis methodology, systematically examining primary military doctrine and secondary academic literature to identify definitional inconsistencies, conceptual gaps, and cross-level incompatibilities in the cyber key terrain concept. The primary source base comprises joint and service-level doctrinal publication: JP 2-01.3, JP 3-12 in its 2018 and 2022 revisions, Air Force Doctrine Publication 3-12, and NATO AJP-3.20 Edition A Version 1 (2020), together with U.S. and NATO strategic documents including the 2023 DoD Cyber Strategy.

The secondary source base comprises peer-reviewed and conference publications from 2001 to 2023 identified through targeted review of the cyber terrain and cyberspace geography literature, following the framework established for distinguishing between the two fields (Grandin 2023). The analysis of expanded cyberspace models draws particularly on Venables (2021), whose eight-layer model represents the most comprehensive academic treatment of cyberspace composition currently available in peer-reviewed literature.

The analytical approach proceeds in three stages:

1. First, doctrinal definitions of cyberspace and cyber key terrain are compared across documents to identify structural inconsistencies, with particular attention to the progressive expansion of cyberspace layer models across joint, NATO, and academic sources.
2. Second, the concept's applicability is assessed at each operational level (tactical, operational, and strategic) against four criteria: *physicality* (the element have a stable, bounded existence), *controllability* (it can be seized, held, or denied), *temporal stability* (it is stable enough to support planning), and *scalability* (concept remain coherent as operational scope expands).
3. Third, the reconciliation framework is developed inductively from the identified gaps, drawing on conceptual frameworks from cyberspace geography (Dodge and Kitchin 2001; Gao et al. 2019; Lü, Yuan, and Yu 2021), graph theory, and social network analysis as sources for alternative models at virtual and cognitive layers. The method follows the doctrinal concept development approach (Raymond et al. 2014; Huntley 2016).

3. RESULTS

3.1. Literature Review: Development of the Cyber Key Terrain Concept

3.1.1. Historical Development of Key Terrain in Physical Domains

The concept of key terrain has deep roots in military thinking. Clausewitz emphasized the importance of geographic position in warfare, and subsequent Western doctrine formalized the idea that certain localities provide decisive advantage. Current U.S. joint doctrine (JP 2-01.3) maintains the same definition (Joint Chiefs of Staff 2009), emphasizing three characteristics: physicality (a locality or area), control (seizure or retention), and advantage (marked benefit to military operations).

Critically, traditional key terrain concepts assume several conditions that may not hold in cyberspace: terrain is relatively static between engagements; terrain can be physically occupied and denied to adversaries; terrain exists independent of human construction; and terrain advantage is primarily spatial and observable. These assumptions guide how militaries identify, seize, and defend key terrain in physical domains. Each is challenged to varying degrees in cyberspace, and each challenge intensifies as operations move from physical toward virtual and cognitive layers.

3.1.2. Evolution of Cyber Terrain Concepts (1998 - Present)

Early applications of terrain concepts to cyberspace focused on network topology and computer network defense. One of the first systematic treatments argued that *"computer networks are spatial simply because they exist in the physical world"*, emphasizing defensive perimeters in direct analogy to city walls and firewalls (Pingel 2003). This physical-centric approach established a pattern that persists in much subsequent work. The concept was further advanced by identifying eight "earthly manifestations" of cyber key terrain, including data centers, Internet service providers, undersea cables, and supply chains (Mills 2012). While the first five are primarily physical, the latter three (international standards bodies, cyber workforce, and innovation) represent intangible strategic factors whose inclusion raises fundamental questions about conceptual boundaries.

The most comprehensive tactical-level treatment developed methodologies for 'mapping the cyber terrain' using the definition already noted above (Bodeau et al. 2013). The most expansive pre-2020 conceptualization proposed a five-layer model encompassing geographic, physical, logical, cyber-persona, and supervisory planes (Raymond et al. 2014). The 2022 revision of JP 3-12 marked significant doctrinal evolution by officially defining expeditionary cyberspace operations as requiring deployment of cyber forces within physical domains (Joint Chiefs of Staff 2022). The most detailed academic decomposition of the cyberspace environment currently available in peer-reviewed literature proposes the eight-layer model noted in the introduction, developed at Tallinn University of Technology, providing a useful benchmark against which to assess the adequacy of doctrinal models (Venables 2021). Australian defense analysis has independently identified the proliferation problem, observing that publicly available allied strategic documents contain no fewer than eight domain models, inconsistent both between and within national doctrines (Wardrop, C. 2020). This confirms that layer proliferation is not merely an academic concern but an operational impediment recognized across allied forces.

3.1.3. Cyberspace Geography and Mapping

Parallel to military developments, academic geographers developed the field of Cyberspace Geography. The foundational work *Mapping Cyberspace* recognized that cyberspace encompasses more than infrastructure, including the spaces created by networked human

interaction (Dodge and Kitchin 2001). A systematic analysis of the terminology observed that the challenge of defining cyber terrain, cyberspace, and the differences between them remains unresolved, with different sources providing incompatible definitions (Grandin 2023). Chinese learning has advanced the concept of *Cyberspace Surveying and Mapping*. Chinese scholarship has advanced two complementary frameworks: a three-domain model of physical, logical, and cognitive levels (Xu et al. 2019), and the "ternary world" framework that positions cyberspace as the connective layer between physical and socio-human worlds (Gao et al. 2019; Lü, Yuan, and Yu 2021). Both align with AJP-3.20's acknowledgement that the information environment encompasses cognitive, virtual, and physical spaces (para. 1.3), while resisting reduction to physical-layer terrain metaphors.

3.1.4. Gaps in Current Conceptualizations

Multiple authors identify significant gaps in cyber terrain conceptualization. Attention to cyber key terrain has been confined primarily to the physical network layer, and the concept applied to cyberspace is considered "necessarily metaphorical" (Huntley 2016). He concludes that the metaphorical quality creates problems at strategic levels, where properties of the source domain (physical terrain) no longer align with properties of the target domain (virtual cyberspace). The concept is primarily linked to mission requirements, making it fundamentally ephemeral and resistant to strategic generalization (Bertoli and Raio 2018), while the temporal dimension has been identified as remarkably underexplored in the literature (Grandin 2023). Significantly, AJP-3.20 (NATO Standardization Office 2020) provides no formal framework for identifying cyber key terrain at any layer, nor does it address the temporal instability of the domain beyond noting that cyberspace is *"in constant flux"* (para. 1.8). This absence in NATO's promulgated doctrine contrasts with the growing academic consensus that expanded cyberspace models require correspondingly expanded terrain identification methodologies.

3.1.5. Non-NATO Doctrinal Perspectives

An assessment of the cyber key terrain concept would be incomplete without acknowledging how non-NATO military powers conceptualize the operational domain in which terrain identification takes place. Two perspectives are particularly instructive: Chinese *information warfare doctrine* and Russian *information confrontation theory*.

Both converge on a conclusion that reinforces the central argument of this paper: that physical-layer terrain thinking is insufficient for operations in the full cognitive and informational scope of modern conflict.

Chinese military doctrine has progressively developed the concept of *"information warfare"* (xinxi hua zhanzheng), which treats information space as a unified operational domain in which technical, cognitive, and psychological dimensions are inseparable (Ye Zheng 2013). The People's Liberation Army (PLA) doctrine of integrated network-electronic warfare combines cyberspace operations with electromagnetic spectrum control and cognitive influence within a single operational concept, explicitly rejecting the separation of technical infrastructure from the informational and psychological effects it enables.

This integration makes physical-layer terrain identification frameworks not merely insufficient, but conceptually incompatible with PLA operational thinking at the strategic level, where the decisive contest is understood to occur in the cognitive dimension. The Chinese academic scholarship on cyberspace geography noted in section 3.1.3, particularly the three-fold world framework (Gao et al. 2019; Lü, Yuan, and Yu 2021) reflects this doctrinal orientation, positioning cyberspace as a connective layer between physical and socio-human worlds rather than as a technical infrastructure amenable to terrain-style mapping.

Russian military theory employs the concept of *"information confrontation"* (informatsionnoe protivoborstvo), which explicitly integrates technical, cognitive, and psychological dimensions into a single operational space (Thomas 2004; Giles 2016). Russian doctrine distinguishes between the technical-informational dimension (focused on data and network infrastructure) and the psychological-informational dimension (focused on perception, decision-making, and morale), treating both as equally legitimate and inseparable theatres of operation.

This two-dimensional framework predates and in some respects anticipates the multi-layer academic models discussed in section 3.1.2, but arrives at an operationally integrated conclusion that NATO doctrine has not yet matched: that operations in the psychological dimension require fundamentally different conceptual tools from those used for technical network operations. From the perspective of the cyber key terrain paradox, Russian information confrontation doctrine effectively dissolves the paradox by abandoning terrain language altogether for the psychological dimension, replacing it with influence-based operational concepts that have no terrain analogue.

These non-NATO perspectives do not resolve the doctrinal challenges identified in this paper, but they confirm that the inadequacy of physical-layer terrain frameworks for higher-layer operations is recognized beyond the Alliance. They also suggest that the reconciliation framework proposed in section 3.4 (which acknowledges the metaphorical limitations of terrain language at cognitive and social dimensions and introduces alternative conceptual models for those layers) is directionally consistent with the operational thinking of peer competitors, even if the specific frameworks differ.

The extent to which the cyber key terrain paradox manifests differently within Chinese and Russian doctrine, and the implications for allied planning in contested information environments, represent important directions for future research beyond the scope of this study.

3.2. The Cyber Key Terrain Paradox: Sources and Structure

3.2.1. Definitional Inconsistency across Doctrinal Documents

The paradox emerges clearly from a comparison of doctrinal definitions. Cyberspace itself is consistently defined as multi-dimensional across all major documents:

- three layers: physical network, logical network, and cyber-persona (JP 3-12 2018, 2022);
- three-layer model: physical, logical, and cyber-persona (AJP-3.20 paras. 1.9-1.12 - NATO Standardization Office 2020);
- five planes (Raymond et al. 2013;
- five layers including cognitive and socio-organizational dimensions (Grant 2014) and
- the most detailed model with eight layers (Venables 2021).

Each model assigns substantial weight to virtual and human elements.

Cyber key terrain, by contrast, is defined across all documents with a predominantly physical emphasis. No NATO-agreed definition of cyber key terrain exists in the current promulgated doctrine. The academic definitions, from "physical and logical elements" (Bodeau et al. 2013) to broader treatment (Raymond et al. 2014) are formally applicable to multiple layers, but practical identification methodologies focus overwhelmingly on the physical and lower logical layers.

AJP-3.20's three-layer model already introduces a structural inconsistency: the cyber-persona layer is formally part of the domain, but the publication provides no framework for identifying terrain at that layer. The information environment concept (para. 1.3), which encompasses cognitive,

virtual, and physical space extends the operational scope further, but again provides no terrain identification methodology. This creates a gap between the recognized scope of cyberspace operations and the conceptual tools available for planning them, a gap that widens as academic models expand the layer count.

Table 1 summarizes the cyberspace layer models examined in this study, illustrating the progressive expansion from the three-layer framework of JP 3-12 and AJP-3.20 to the eight-layer model proposed by Venables (2021).

3.2.2. The Layer Problem

The proliferation of cyberspace layer models compounds definitional challenges. JP 3-12 and AJP-3.20 divides cyberspace into physical network, logical network, and cyber-persona layers. Raymond et al. (2014) and Grant (2014) add geographic or supervisory/ cognitive planes. Venables (2021) explicitly incorporate geographic, infrastructure, syntactic, semantic, and services dimensions alongside the persona layer, and notes that *"it is vital that there is a comprehensive understanding of the properties of the seven layers of cyberspace, the users active in it, and their mission."* This proliferation is not confined to NATO-level doctrine.

Table 1. Comparison of Cyberspace Layer Models in Military Doctrine and Academic Literature.

Source	Year	No. of Layers	Layer Names	Cognitive / Social included
JP 3-12 / AJP-3.20	2018-2022 / 2020	3	Physical network; Logical network; Cyber-persona	**No** (acknowledged in IE concept only)
Raymond et al.	2014	5	Geographic; Physical; Logical; Cyber-persona; Supervisory	**Partial** (supervisory layer)
Grant	2014	5	Physical; Logical; Cyber-persona; Cognitive; Socio-organizational	**Yes**

Source	Year	No. of Layers	Layer Names	Cognitive / Social included
Venables	2021	8	Geographic; Physical; Infrastructure; Syntactic; Semantic; Services; Persona; Mission	**Yes** (persona, semantic, mission layers)

Source: Author

National approaches add further variation: the UK's JDN 1/18 on Cyber and Electromagnetic Activities (CEMA) frames cyberspace within the broader electromagnetic environment, emphasizing the convergence of cyber and electromagnetic activities as an integrated operational challenge (UK Ministry of Defence 2018). Australia's ADF-C-0 defines the cyber domain as comprising *"cyberspace and the electromagnetic spectrum"* and has established separate career tracks for cognitive and information warfare distinct from cyber operations (Australian Department of Defence 2024). Germany's Bundeswehr elevated its Cyber and Information Domain Service (Cyber- und Informationsraum, CIR) to a full military service branch in 2024, explicitly combining cyberspace with the broader information domain.

Each national approach implicitly acknowledges that the technical three-layer model of cyberspace is insufficient for operational purposes, yet each extends it in a different direction: the UK toward electromagnetic convergence, Australia toward cognitive warfare, Germany toward information space integration, further complicating the interoperability challenge.

For cyber key terrain conceptualization, this expanding proliferation of layer models intensifies the existing problem. If different documents disagree on whether cyberspace has three, five, or eight layers, no systematic determination of what constitutes key terrain at each layer is possible across the Alliance. AJP-3.20's three-layer model does not resolve the conceptual gap; rather, the academic literature demonstrates that adding cognitive, social, and semantic layers (as the expanded models do) widens it, because these layers have no established key terrain identification methodology of any kind.

The confusion may partly explain why most practical discussions continue to retreat to

the physical dimension, where consensus is easiest: everyone agrees routers, cables, and servers are part of cyberspace, even if they disagree about how to treat influence networks or cognitive manipulation as terrain.

3.2.3. Temporal Dimensions and Dynamic Terrain

A crucial but underdeveloped dimension of the cyber key terrain paradox concerns *temporality*. Traditional terrain is relatively static, hills do not move between battles, and rivers follow predictable courses. Cyberspace changes continuously at multiple timescales. Grandin (2023) identifies this gap explicitly, noting that *"it is remarkable how little the temporal aspect of cyberspace, and how time affects the different levels or planes, is covered in research."* AJP-3.20 acknowledges that cyberspace is *"in constant flux"* (para. 1.8), but provides no systematic framework for addressing temporal instability in operational planning.

The temporal challenge manifests differently across layers. Physical infrastructure elements (the focus of AJP-3.20's physical layer) change over months or years, while logical layer elements (operating systems, protocols, applications - para. 1.11) change more rapidly. The cyber-persona layer (para. 1.12) is still more volatile: virtual identities can be created, modified, or abandoned in hours.

The cognitive and social dimensions identified by Grant (2014) and Venables (2021) operate at even higher tempos: influence campaigns shift over days, and cognitive states change in response to operational information pressure. Cyber key terrain is temporally linked to specific missions even at the tactical level: what is key for one operation may be irrelevant for the next (Bertoli and Raio 2018; Franz 2012). The multi-timescale instability means that temporal classification cannot be uniform across layers, and doctrine must explicitly account for the different reassessment cycles each dimension requires.

3.3. Cross-Level Assessment

3.3.1. Tactical Level: Where the Concept Works

At the tactical level, focused on specific missions and near-term objectives, the cyber key terrain concept demonstrates its greatest utility and consistency. Even without a formal NATO-agreed definition, the concept operates effectively when applied to physical and lower logical layer elements. The approach described in the academic literature (a systematic inventory of mission-

relevant cyber assets, identification of critical nodes, and prioritization for defensive effort (Bodeau, Graubart, and Heinbockel 2013; Guion and Reith 2017; Price et al. 2017) provides a structured, mission-focused methodology that tactical commanders can apply within the AJP-3.20 framework of defensive and offensive cyberspace operations (paras. 2.19–2.24).

Tactical applications concentrate on mission-specific network defense and attack operations where physical and lower virtual layer elements dominate. Jakobson (2011) provides a representative model with hardware, software, and service sub-terrains, each inventoried and assessed for criticality. Guion and Reith (2017) developed tools for tactical cyber terrain mission mapping using subject matter expert evaluation. Price et al. (2017) demonstrate the approach in mission reconfigurable cyber systems. Youn et al. (2021) extend this line of work by applying BGP archive data to Cyber Intelligence Preparation of the Battlefield (IPB), producing network-based situational awareness visualizations that support key terrain identification at the tactical level.

The physical layer emphasis at tactical level succeeds because it aligns with four operational factors: *immediacy* (physical infrastructure directly enables or prevents mission execution); *observability* (physical elements can be discovered and monitored); *controllability* (physical assets can be defended, secured, or destroyed); and *predictability* (physical elements behave according to known technical parameters).

The effective management of these physical infrastructure elements requires specialized competencies in critical infrastructure governance, as cyber infrastructure systems demand mature management frameworks that address technical, organizational, and strategic dimensions simultaneously (Codreanu 2020).

Table 2 applies the four analytical criteria established in the Methodology to each operational level, making visible the structural degradation of the terrain metaphor as the scope of operations expands.

3.3.2. Operational Level: Where Complexity Begins

At the operational level (concerned with campaigns rather than discrete missions) cyber key terrain identification becomes significantly more complex. The timeframe extends from hours or days to weeks or months; the scope encompasses entire theatre-level networks; and the terrain must support multiple missions with potentially conflicting requirements.

Table 2. Cross-Level Assessment of the Cyber Key Terrain Concept against Four Criteria.

Operational Level	Physicality	Controllability	Temporal Stability	Scalability
Tactical	**High** (physical infrastructure directly enables mission execution)	**High** (assets can be defended, secured, or destroyed)	**Adequate** (physical elements change over months/years)	**Limited to mission scope**; SME evaluation works at this scale
Operational	**Moderate** (logical and persona layers become relevant across campaigns)	**Partial** (logical elements controllable; persona layer less so)	**Reduced** (logical layer changes faster; update cycles conflict)	**Strained** (SME methodology does not scale to theatre-level complexity)
Strategic	**Low** (cognitive and social dimensions dominate; no geographic fixity)	**Fails** (cognitive/ narrative spaces cannot be seized or held)	**Absent** (influence campaigns shift over days; no doctrinal reassessment cycle)	**Fails** (terrain concept loses coherence; no strategic identification framework)

Source: author

Physical layer elements retain importance, but logical and persona layers become increasingly relevant as operations span longer periods and broader objectives. AJP-3.20 acknowledges the operational dimension of cyberspace through its treatment of joint functions (paras. 1.23-1.35), noting that cyberspace operations *"may support other operations or achieve operational objectives by itself"* and that *"effects by COs are synchronized with other effects and capabilities of the overall operation to create synergy"* (para. 1.23).

The challenge is that subject matter expert evaluation (the primary methodology at tactical level) does not scale adequately to the operational level's complexity. Huntley (2016) identifies this scalability problem as a central limitation of existing conceptualizations. The absence of formal cyber key terrain frameworks in AJP-3.20 means that operational planners lack doctrinal guidance for systematic terrain identification

across even the three recognized layers, let alone the expanded models proposed in academic literature. How to conduct systematic key terrain identification in the logical or persona layers at campaign scale, or how to manage the different update cycles those layers require, remains an open methodological question.

Modern operational doctrine increasingly emphasizes multi-domain operations (MDO), in which cyber effects must be synchronized with air, land, maritime, and space operations. AJP-3.20 addresses cross-domain synchronization through its joint functions framework, noting that cyberspace operations must be coordinated with electromagnetic operations (para. 1.29), intelligence (para. 1.31), and information activities (para. 1.32).

The Atlantic Council (2024) has assessed NATO's progress toward multi-domain integration. However, coherent conceptual agreement on MDO implementation across the Alliance remains incomplete. The UK's CEMA concept (UK Ministry of Defence 2018) represents one national attempt to address this integration challenge, emphasizing the synchronization of cyber and electromagnetic activities to deliver operational advantage, but it does not resolve the underlying terrain identification problem across the higher layers. This gap is partly a reflection of the unresolved cyber key terrain paradox: without coherent concepts of decisive cyber positions across all layers and all levels, meaningful integration with other domains remains aspirational rather than systematic.

3.3.3. Strategic Level: Where the Concept Breaks Down

At the strategic level, concerned with achieving national objectives, allocating resources across theatres, and shaping long-term capabilities, contradictions between cyber key terrain definitions and requirements become acute. Huntley (2016) documented the pattern of strategic documents avoiding the cyber key terrain term across successive U.S. DoD strategy documents, a pattern that continues through the 2023 DoD Cyber Strategy. AJP-3.20's three-layer model provides no strategic-level terrain identification framework, and the publication's planning and conduct guidance (Chapter 3) focuses on operational-level considerations, without addressing what key terrain identification looks like when applied to the cyber-persona layer at strategic scale, let alone to the cognitive and social dimensions identified in the broader IE concept (para. 1.3).

The cognitive and social dimensions, which AJP-3.20 acknowledges through its information environment formulation (para. 1.3) and its treatment of the information function (para. 1.32), present the

sharpest challenge. AJP-3.20 notes that the IE encompasses *"cognitive, virtual and physical space"* (para. 1.3) and that information activities seek to *"influence relevant actor perceptions, behavior, action or inaction and decision making"* (para. 1.32).

These are the spaces where influence operations, disinformation campaigns, and strategic narrative competition occur. JP 3-12 defines the cyber-persona layer similarly. Raymond et al. (2014) identify some persona-layer key terrain elements (administrator accounts, political leader accounts), but these treat personas as technical access points rather than engaging the strategic challenge of population-scale influence networks. Australia's recent establishment of dedicated cognitive and information warfare career tracks within the ADF (Australian Department of Defence 2024) represents an institutional recognition that operations in the cognitive dimension require fundamentally different skills and frameworks from those used for technical cyberspace operations, a distinction that terrain-based conceptualizations do not currently accommodate.

Venables (2021) explicitly separates persona, services, and semantic layers, demonstrating that the human-interaction dimensions of cyberspace are analytically distinct from the technical infrastructure, yet no terrain identification framework exists for any of them.

Mills (2012) expands cyber key terrain to include workforce, innovation capacity, and international standards bodies. These elements fail the core criteria of traditional terrain: they cannot be seized through military operations, they lack geographic location or topological position, and they relate to military capabilities through causal chains spanning decades. If cyber terrain is expanded to include all factors affecting cyber capabilities, the concept loses analytical utility. AJP-3.20's civil-military cooperation section acknowledges the boundary problem: cyberspace *"allows commanders to establish information links with civilian counterparts"* and cooperation can improve *"cyber security"* of civilian actors (para. 1.35), recognizing that operationally significant terrain elements in cyberspace are often outside the direct control of the military.

At strategic levels, the national security implications multiply: without coherent strategic terrain concepts, militaries lack frameworks for prioritizing long-term cyber investments, and doctrinal gaps cascade downward, creating confusion about priorities, authorities, and methods at lower levels.

3.4. The Reconciliation Framework

3.4.1. Acknowledging the Metaphorical Nature of Cyber Terrain

The foundation of the proposed reconciliation framework is explicit acknowledgement that cyber key terrain is, as Huntley (2016) concludes, *"necessarily metaphorical."* Metaphors work by transferring understanding from familiar domains to less familiar ones. For physical cyber infrastructure and tactical operations, the alignment between source and target domain is sufficient for the terrain metaphor to generate useful analytical insights; the academic literature on tactical cyber terrain mapping is evidence of this utility (Bodeau, Graubart, and Heinbockel 2013; Guion and Reith 2017).

For the logical and persona layers at operational scale, and for the cognitive and social dimensions at any level, the alignment breaks down in ways that current doctrine does not acknowledge. AJP-3.20's IE formulation (para. 1.3), by explicitly acknowledging cognitive and virtual spaces as operationally significant, implicitly recognizes these dimensions, but provides no terrain framework for them, leaving practitioners with a conceptual gap precisely where strategic effects are increasingly contested.

3.4.2. Adaptive Layer-Specific Definitions

Rather than seeking one universal definition, doctrine should provide adaptive definitions that vary by operational level and cyberspace layer.

At the ***tactical physical dimension*** (AJP-3.20's physical layer, para. 1.10): *cyber key terrain consists of network infrastructure, devices, and physical connections whose control or denial would immediately and significantly affect mission accomplishment within a defined operational timeframe*.

At the ***tactical virtual dimension*** (AJP-3.20's logical and cyber-persona layers, paras. 1.11–1.12): *key terrain consists of software systems, data repositories, logical network configurations, and digital identities whose exploitation, control, or disruption would provide marked tactical advantage in achieving specific mission objectives*.

At the ***operational physical dimension***: *cyber key terrain consists of infrastructure and network systems whose sustained control enables campaign operations, serves as necessary foundation for multiple tactical operations, or whose loss would require significant operational adaptation, including expeditionary cyber capabilities required for operations against isolated networks* (Joint Chiefs of Staff 2022).

At the ***operational virtual dimension***: *key terrain consists of software architectures, data systems, protocol implementations, and influence network positions whose control enables sustained offensive or defensive operations, facilitates multi-domain integration, or whose compromise would produce cascading operational effects*.

At the ***strategic physical dimension***: *cyber key terrain consists of critical infrastructure whose control affects national cyber capabilities or enables long-term strategic operations, including infrastructure outside direct military control requiring civil-military coordination* (AJP-3.20 para. 1.35).

At the ***strategic virtual and cognitive dimensions:*** the framework explicitly acknowledges that the terrain metaphor is severely strained for the cognitive and social spaces identified in AJP-3.20's IE concept (para. 1.3). The information function's emphasis on influencing *"relevant actor perceptions, behavior, action or inaction and decision making"* (para. 1.32) indicates that alternative conceptual models (influence topology mapping, social network centrality analysis, narrative space models) may provide superior operational understanding at these layers than terrain metaphors. Terrain language may be preserved for doctrinal continuity, but practitioners must understand its metaphorical limitations in these contexts.

3.4.3. Temporal Classification

Building on AJP-3.20's acknowledgement that cyberspace is "in constant flux" and "constantly under development" (para. 1.8), doctrine must incorporate an explicit temporal classification across all layers. Static elements (geographic infrastructure locations, submarine cables, major data centers) change over years and warrant annual reassessment (these correspond to the physical layer in AJP-3.20) (para. 1.10). Semi-static elements (physical network configurations, installed software, established protocols) change over months and warrant quarterly review. Dynamic elements (active vulnerabilities, authentication credentials, cloud configurations) change over weeks and require monthly assessment or intelligence-triggered updates. Highly dynamic elements (persona profiles, social media presence, current influence campaigns) change over days and require continuous monitoring, a timescale for which no systematic NATO doctrine currently exists. The temporal instability of cognitive-layer terrain, which changes at human psychological rates under operational information pressure, is the most analytically challenging and the most under addressed in current doctrine.

Table 3 presents the temporal classification framework above, specifying reassessment cycles

calibrated to each layer's actual rate of change and its correspondence to AJP-3.20's layer model.

Table 3. Temporal Classification of Cyber Terrain Elements across AJP-3.20 Layers.

Category	Example Elements	Rate of Change	Reassessment Cycle	AJP-3.20 Layer Correspondence
Static	Geographic infrastructure locations, submarine cables, major data centers	Years	Annual	Physical layer (para. 1.10)
Semi-static	Physical network configurations, installed software, established protocols	Months	Quarterly	Physical / lower Logical (paras. 1.10–1.11)
Dynamic	Active vulnerabilities, authentication credentials, cloud configurations	Weeks	Monthly or intelligence-triggered	Logical layer (para. 1.11)
Highly dynamic	Persona profiles, social media presence, active influence campaigns	Days	Continuous monitoring	Cyber-persona / Cognitive IE (paras. 1.12, 1.3)

Source: author

3.4.4. Context-Dependent Identification Methodology

A practical methodology for cyber key terrain identification must be context-dependent, extending the planning processes described in AJP-3.20 Chapter 3 to address all recognized cyberspace layers and the broader IE dimensions. The following eight-step process provides a structured approach consistent with AJP-3.20's operations planning process (paras. 3.18–3.26) while addressing the limitations identified in this study.

- ***Step 1*** defines the operational context: level (tactical, operational, strategic), mission type (offensive, defensive, intelligence, or influence), and relevant timeframe, with explicit identification of which cyberspace layers and IE dimensions are implicated.
- ***Step 2*** identifies the relevant cyberspace layers across the AJP-3.20 three-layer model and, where operationally appropriate, the expanded layers proposed in academic

literature.

- ***Step 3*** applies layer-specific identification methods: network mapping and infrastructure assessment for the physical layer; software dependency analysis and vulnerability assessment for the logical layer; social network analysis and influence mapping for the cyber-persona layer and the cognitive/social dimensions of the IE.
- ***Step 4*** applies criticality metrics appropriate to the operational level.
- ***Step 5*** assesses temporal factors using the classification above, determining validity periods and establishing update schedules calibrated to each layer's actual rate of change.
- ***Step 6*** documents the metaphorical limitations of terrain language for the layers under assessment, particularly at operational and strategic levels for virtual and cognitive dimensions, and notes where alternative frameworks supplement terrain analysis.
- ***Step 7*** integrates the terrain assessment into the AJP-3.20 planning process (the informing course of action development - para. 3.22), supporting risk management (paras. 3.27-3.29), and coordinating across domains and authorities, including civil-military coordination for infrastructure outside direct military control (para. 1.35).
- ***Step 8*** establishes continuous assessment and adaptation, recognizing that cyber terrain requires ongoing monitoring matched to each layer's temporal classification rather than the periodic static studies appropriate to physical terrain.
- Figure 1 presents the eight-step context-dependent identification methodology proposed in section 3.4.4, illustrating the sequential process and the continuous feedback loop between Step 8 and Step 1 that reflects the dynamic nature of cyber terrain.

3.4.5 Criticality Metrics across Levels

Defining "key" terrain requires metrics of criticality across operational levels. At the *tactical level*, relevant metrics include mission dependency (does this element directly enable mission-essential functions), redundancy (are alternative elements available), recovery time, and access control difficulty. At the *operational level*, metrics include campaign criticality, cascade potential, integration significance for multi-domain synchronization, and adaptation timeframe if the element is lost.

Fig. 1. Eight-Step Context-Dependent Cyber Key Terrain Identification Methodology (adapted from AJP-3.20 planning process, paras. 3.18-3.26)

At the *strategic level*, metrics include national capability impact, international implications, long-term significance, and economic and political consequences. For *virtual and cognitive layers at strategic level*, influence metrics (narrative reach, audience penetration, credibility position, community centrality) supplement or replace traditional terrain control metrics. These adapted metrics reflect the fundamental difference between controlling a physical node and achieving advantage in a cognitive or social space.

Table 4 consolidates the criticality metrics above, organizing them by operational level and distinguishing physical-layer metrics from those applicable to virtual and cognitive dimensions.

Table 4. Criticality Metrics for Cyber Key Terrain Identification across Operational Levels.

Metric Category	Tactical Level	Operational Level	Strategic Level
Primary focus	Mission-essential functions	Campaign continuity	National cyber capability
Key metrics	Mission dependency; redundancy; recovery time; access control difficulty	Campaign criticality; cascade potential; MDO integration significance; adaptation timeframe	National capability impact; international implications; long-term significance; economic and political consequences
Virtual / cognitive layer metrics	Not applicable at tactical physical focus	Influence network position; protocol control; data architecture access	Narrative reach; audience penetration; credibility position; community centrality
Primary identification method	Subject matter expert evaluation; network mapping	Dependency analysis; vulnerability assessment at scale	Social network analysis; influence topology mapping; graph-theoretic models

Source: author

3.5. Alternative Conceptual Frameworks for Virtual and Cognitive Layers

The recognition that the information environment encompasses cognitive, virtual, and physical spaces (AJP-3.20 para. 1.3), combined with the progressive expansion of cyberspace models in academic literature, and creates a doctrinal imperative for alternative conceptual frameworks that are native to the virtual and cognitive dimensions. For the logical layer, architectural and graph-theoretic models analyze network centrality, connectivity, and shortest paths, providing rigorous analytical grounding that terrain metaphors lack. Ecosystem models capture cascading failures and systemic vulnerabilities, consistent with AJP-3.20's concern with cascading effects in cyberspace operations (para. 2.28). Economic models of bottlenecks and critical dependencies offer additional analytical purchase.

For the cyber-persona layer (AJP-3.20 para. 1.12) and the cognitive and social dimensions of the IE, the terrain metaphor becomes analytically deceptive at operational and strategic scale. Social network models identify influencers, connectors, and bridges between communities, while market-share models frame competition for attention, credibility, and narrative dominance. Epidemiological models track information spread and viral dynamics, while game-theoretic models analyze strategic interactions and reputation dynamics.

These frameworks are native to the properties of the virtual and cognitive environment and are better aligned with the analytical methods of the social and cognitive sciences, whose expertise is increasingly relevant to cyber operations at these layers.

AJP-3.20 itself implicitly acknowledges this need through its treatment of the information function (para. 1.32), identifying Strategic Communications, Information Operations, Psychological Operations, and Military Public Affairs as key enablers. These descriptions call for social network analysis, audience segmentation, and cognitive influence modelling, not terrain identification. The doctrinal implication is not to abandon terrain language entirely (its familiarity and genuine utility at the physical dimension are assets worth preserving) but to treat terrain thinking as one framework among several, appropriate to specific layers and levels, supplemented explicitly by alternative models where its assumptions do not hold.

Each of these alternative frameworks offers distinct analytical capabilities and carries specific limitations that operational planners must understand.

For the logical layer, ***graph-theoretic centrality models*** identify which network nodes lie on the most critical communication paths, providing a mathematically rigorous basis for prioritization that terrain

metaphors cannot supply. Two measures are particularly relevant: *betweenness centrality*, which quantifies how frequently a node appears on shortest paths between other nodes, and *eigenvector centrality*, which weights a node's importance by the connectivity of its neighbors. A node with high betweenness centrality is analytically analogous to key terrain in the sense that its removal would disproportionately disrupt network function, but the concept is defined relationally rather than spatially, and it changes as the network topology evolves. The primary limitation is the assumption of topological stability: centrality measures become unreliable in rapidly reconfiguring networks, which is precisely the environment in which cyber operations occur.

Ecosystem models address this partially by modelling cascading failure dynamics, but they require detailed knowledge of interdependencies that may not be available in adversarial contexts.

For the cyber-persona layer, ***social network analysis (SNA)*** provides concrete metrics (degree centrality, clustering coefficient, and bridging coefficient) that identify key influencers, community connectors, and information brokers within a target population. In an influence operation context, an account with high bridging centrality that connects otherwise disconnected communities occupies a position functionally analogous to key terrain: its compromise or co-option would provide marked advantage in shaping information flows across the network.

The critical limitation of SNA in this context is that it captures structural position but not content, credibility, or narrative resonance: a structurally central account that loses credibility may retain its network position while losing its operational significance, a dynamic that terrain metaphors cannot adequately model. SNA must therefore be combined with content analysis and audience segmentation to provide operationally useful assessments.

Epidemiological models (adapted from the SIR - Susceptible-Infected-Recovered) framework used in disease modelling) offer a powerful approach to tracking information spread and estimating the reach of disinformation campaigns. The *basic reproduction number* (R_0) concept, when adapted to information spread, provides planners with an estimate of how many additional actors a given narrative will reach from each exposed individual, enabling assessment of viral dynamics before an operation reaches saturation.

The principal limitation is the assumption of population homogeneity: unlike biological pathogens, information spread is highly sensitive to individual credibility assessments, prior beliefs, and community membership, factors that require significant empirical calibration to model accurately.

Game-theoretic models, finally, provide analytical purchase on strategic interactions where outcomes depend on the choices of multiple actors, particularly useful for modelling credibility dynamics, deterrence signaling, and reputation competition in the cognitive domain. Their principal limitation is the requirement for specified payoff structures that are rarely available with precision in operational contexts, making them more useful for conceptual analysis than for tactical planning.

These limitations do not diminish the utility of the proposed frameworks relative to terrain metaphors, but rather underscore the need for a multi-framework approach in which no single conceptual model is treated as universally applicable. The practical implication for doctrine is that the selection of analytical framework should be driven by the operational layer, the temporal classification of the terrain elements under assessment, and the specific planning question being addressed (precisely the context-dependent approach formalized in the eight-step methodology proposed in section 3.4.4.).

4. DISCUSSION

4.1. Interpreting the Paradox

The cyber key terrain paradox (the systematic degradation of the concept's utility as operations move from physical-layer tactical applications toward virtual and cognitive layer strategic ones) is not a peripheral doctrinal curiosity. It reflects a fundamental challenge in adapting centuries of military spatial thinking to a domain that is partially but not wholly spatial. A critical finding of this analysis is that the paradox is already present within AJP-3.20's three-layer model: the cyber-persona layer (para. 1.12) already strains the terrain metaphor, since virtual identities lack the physical properties that terrain concepts assume. The expanded models proposed in academic literature (particularly Venables's eight-layer model and Grant's cognitive dimensions) intensify the paradox further, by formally incorporating layers for which no terrain identification methodology exists.

The findings confirm Huntley's (2016) assessment that the concept is necessarily metaphorical, while specifying more precisely where the metaphor holds and where it fails. The metaphor holds well at the physical layer across all operational levels. It begins to struggle at the logical and cyber-persona layers, particularly at operational and strategic scales. It fails in the cognitive and social dimensions of the IE, where the concept of seizing or retaining a decisive position has no meaningful analogue in environments characterized by mass-scale influence, shifting narratives, and psychological effects on human decision-making. The absence of a formal NATO-agreed cyber

key terrain definition in AJP-3.20 (and the corresponding absence of terrain identification frameworks for any layer) may itself be a tacit acknowledgement that the Alliance has not yet resolved these conceptual challenges.

4.2. Doctrinal Recommendations

Several specific doctrinal recommendations follow from this analysis. First, NATO doctrine should develop and promulgate formal definitions for cyber key terrain, mission-relevant terrain in cyberspace, and an associated prioritized asset list, concepts that exist in academic literature (Raymond et al. 2014; Bodeau et al. 2013) and U.S. doctrine but are absent from AJP-3.20. These definitions should explicitly acknowledge the metaphorical nature of terrain concepts beyond the physical and lower logical layers, and state clearly that current identification methodologies do not extend to the cognitive and social dimensions of the IE.

Second, temporal classification should be formally incorporated into any cyber terrain framework, with explicit guidance on update cycles calibrated to each layer's rate of change. Third, NATO doctrine should either develop terrain identification methodologies specifically addressing the cyber-persona layer and the cognitive/social dimensions of the IE, or explicitly acknowledge that terrain language is unsuitable at those layers and introduce alternative conceptual frameworks (social network analysis, influence topology mapping) as primary analytical tools for operations in those dimensions.

Fourth, JP 3-12 and AJP-3.20 should be reconciled on layer models. The current three-layer alignment provides formal interoperability but masks a growing consensus that additional layers are operationally significant. Key allies have already moved beyond this model in their national force structures (the UK through CEMA, Australia through cognitive and information warfare integration, and Germany through the Cyber and Information Domain Service) creating de facto interoperability gaps that formal NATO doctrine does not yet address.

4.3 Implications for Operational Planning

For operational planners, the reconciliation framework has several practical implications. Planning processes should explicitly distinguish between terrain assessment at the physical, logical, and cyber-persona layers of AJP-3.20, and in the broader cognitive and social dimensions of the IE, applying appropriate methodologies and criticality metrics to each. Terrain assessments should always specify their temporal scope and validity period, with update mechanisms calibrated to the temporal classification of each layer.

Multi-domain operations planning should integrate cyber terrain assessment across all

recognized layers, not only the physical dimension, to support meaningful synchronization with other domains and with the non-military instruments of power that contemporary doctrine requires. Practical guidance for bridging joint doctrine and operational planning in this domain is available in the U.S. Army War College Strategic Cyberspace Operations Primer (U.S. Army War College 2023), which synthesizes joint and service doctrine into a planning-oriented reference applicable across command levels.

For allied and combined operations, the definitional inconsistencies documented in this paper argue for urgent development of NATO Standardization Agreements covering cyber terrain identification methodologies across all layers. The existing AJP-3.20 terminology (para. 1.13) (cyberspace, cyberspace operation, defensive and offensive cyberspace operations, cyber security, mission assurance) provides a foundation, but cyber key terrain and associated concepts require formal NATO-agreed definitions and methodological guidance.

4.4. Implications for Professional Military Education

The concepts proposed here require integration into professional military education at all levels. Officers must understand both the genuine tactical utility of physical-layer terrain concepts and the metaphorical limitations of terrain thinking in the virtual and cognitive dimensions. Curricula should introduce the layer models, layer-specific definitions, and alternative frameworks proposed in this study. Exercises should practice terrain identification at tactical, operational, and strategic levels with appropriate variation in methodology and metrics.

The cross-level planning dimension (understanding how tactical terrain assessment feeds operational planning and how operational priorities relate to strategic requirements across all layers) is particularly important and currently tempered in existing training frameworks. Additionally, education programmes should address the divergent national approaches to cyberspace conceptualization among key allies, ensuring that officers understand how different layer models and organizational structures (such as the UK's CEMA integration, Australia's cognitive warfare separation, and Germany's information domain service model) affect planning interoperability in coalition operations.

4.5. Limitations and Future Research Directions

The reconciliation framework proposed in this study is developed through doctrinal and conceptual analysis, which, while consistent with the methodology employed, means that empirical or operational validation remains a next step. Testing the framework against real-world planning requirements

through case studies, simulations, or operational examples would further strengthen its practical applicability.

While this is consistent with the doctrinal concept development methodology employed (Raymond et al. 2014; Huntley 2016), it means that the practical utility of the proposed layer-specific definitions, temporal classification, and eight-step identification methodology remains to be demonstrated in operational contexts. The alternative conceptual models proposed for virtual and cognitive layers (social network analysis, influence topology mapping, and graph theoretic approaches) have established methodological foundations in their source disciplines but have not been empirically validated as planning tools in military cyber operations contexts. Applying the framework to a documented cyber campaign (such as the 2007 Estonia incidents, the 2015-2016 Ukrainian power grid attacks, or the cognitive dimension operations associated with recent hybrid warfare cases) would constitute the most direct form of validation and is identified as the primary direction for future research.

A further limitation is that, despite the addition of non-NATO perspectives in section 3.1.5, the study remains primarily grounded in U.S. and NATO doctrinal sources. The extent to which the paradox manifests differently within Chinese and Russian doctrine, and the operational implications for allied planning in contested information environments, merit deeper separate investigation. These represent the primary directions for future research, alongside the development of practical tools for multi-layer terrain mapping and the empirical testing of criticality metrics against operational outcomes.

5. CONCLUSIONS

The reconciliation framework proposed here does not resolve the fundamental tension between spatial military thinking and the non-spatial dimensions of cyberspace, but it underlines that tension explicitly. The framework preserves the genuine utility of terrain thinking while preventing its misapplication through four integrated contributions: layer-specific and level-specific adaptive definitions, a temporal classification system that extends AJP-3.20's recognition of cyberspace dynamism, a structured identification methodology integrated with AJP-3.20's planning processes, and explicit alternative conceptual frameworks for the cognitive and social dimensions that current doctrine leaves unaddressed. The goal is not to achieve conceptual elegance but doctrinal coherence: a set of frameworks that military planners can apply across the full range of cyberspace operations, from tactical network defense to strategic cognitive dimension competition.

This study makes three principal contributions to military cyber doctrine. First, it provides a systematic cross-level documentation

of the cyber key terrain paradox, demonstrating that the concept's degradation from tactical to strategic levels is structural, predictable, and already manifest within AJP-3.20's three-layer model. Also, it identifies the temporal instability of cyberspace as a cross-cutting dimension of the paradox that current doctrine addresses only in general terms, without providing systematic frameworks for managing different rates of change across layers. Furthermore, it proposes a reconciliation framework that preserves the tactical utility of terrain thinking, while providing the doctrinal coherence that operational and strategic planning across all layers requires.

The most urgent practical implication is the need to develop formal NATO-agreed definitions for cyber key terrain and associated concepts, and to supplement these with explicit guidance for the cyber-persona layer and the cognitive and social dimensions of the information environment.

Addressing the gap between the recognized multi-dimensional character of cyberspace and the predominantly physical-centric terrain frameworks currently available would meaningfully advance military planning across the full scope of cyberspace operations, and in particular support the integration of cognitive dimension operations into multi-domain approaches.

DATA AVAILABILITY STATEMENT

All data supporting the findings of this study are included in the manuscript. The analysis is based exclusively on publicly available military doctrine and peer-reviewed academic literature cited in the references.

AI DISCLOSURE

During the preparation of this work, the author used AI-assisted writing tools to support structural organization and language editing. All substantive analytical content, doctrinal interpretations, and conclusions are the author's own. The author reviewed and edited all AI-assisted content and takes full responsibility for the accuracy and integrity of the published work.

REFERENCES

[1] Atlantic Council. 2024. NATO Multidomain Operations: Assessment and Recommendations. Washington, DC: Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2024/03/NATO-multidomain-operations-Near-and-medium-term-priority-initiatives.pdf

[2] Wardrop, C. 2020. "Victory in the Age of Cyber-Enabled Warfare." Future Forge. Canberra: Australian Army Research Centre. https://theforge.defence.gov.au/publications/victory-age-cyber-enabled-warfare

[3] Australian Department of Defence. 2024. ADF-C-0: Australian Military Power. Edition 2. Canberra: Department of Defence.

[4] Bertoli, G., and S. Raio. 2018. "The Elusive Nature of Cyber Terrain." Journal of Cyber Security and Information Systems: 40-47.

[5] Bodeau, D., R. Graubart, and W. Heinbockel. 2013. Mapping the Cyber Terrain. Bedford, MA: The MITRE Corporation. https://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf

[6] Codreanu, A. 2020. "Competențe necesare gestionării infrastructurilor critice" [Competencies Required for Critical Infrastructure Management]. In Managementul Capabilităților și capabilitatea managerială în cadrul sistemelor de infrastructuri critice, edited by Dorel Badea, Olga Bucoveţchi, and Dumitru Iancu, 90-104. Sibiu: Editura Academiei Forțelor Terestre "Nicolae Bălcescu."

[7] Department of the Air Force. 2021. Air Force Doctrine Publication 3-12: Cyberspace Operations. Washington, DC: Department of the Air Force. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf

[8] Dodge, M., and R. Kitchin. 2001. Mapping Cyberspace. London: Routledge. https://doi.org/10.4324/9780203165270

[9] Development, Concepts and Doctrine Centre. 2022. Cyber Primer. 3rd ed. Shrivenham, UK: UK Ministry of Defence. https://www.gov.uk/government/publications/cyber-primer

[10] Franz III, G. J. 2012. "Effective Synchronization and Integration of Effects through Cyberspace for the Joint Warfighter." Presentation at AFCEA TechNetLand Forces-East Conference, Baltimore, MD, August.

[11] Gao, C., Q. Guo, D. Jiang, Z. Wang, C. Fang, and M. Hao. 2019. "Theoretical Basis and Technical Methods of Cyberspace Geography." Journal of Geographical Sciences 29: 1949–1964. https://doi.org/10.1007/s11442-019-1698-7

[12] Giles, K. 2016. Handbook of Russian Information Warfare. Rome: NATO Defense College. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf

[13] Grandin, A. 2023. "Cyberspace Geography and Cyber Terrain: Challenges in Producing a Universal Map of Cyberspace." In Proceedings of the 22nd European Conference on Cyber Warfare and Security, 207-213. https://papers.academic-conferences.org/index.php/eccws/article/view/1255

[14] Grant, T. 2014. "On the Military Geography of Cyberspace." In Proceedings of the 9th International

Conference on Cyber Warfare & Security, 66-76. Purdue University.

[15] Guion, J., and M. Reith. 2017. "Cyber Terrain Mission Mapping: Tools and Methodologies." In 2017 International Conference on Cyber Conflict, 105–111. Washington, D.C.: IEEE. https://doi.org/10.1109/CYCONUS.2017.8167504

[16] Huntley, W. L. 2016. Cyber Key Terrain: A Conceptual Assessment. Monterey, CA: U.S. Naval Postgraduate School. https://apps.dtic.mil/sti/trecms/pdf/AD1111645.pdf

[17] Jakobson, G. 2011. "Mission Cyber Security Situation Assessment Using Impact Dependency Graphs." In 14th International Conference on Information Fusion, 1–8. Chicago, IL: IEEE. https://ieeexplore.ieee.org/document/5977648

[18] Joint Chiefs of Staff. 2009. Joint Publication 2-01.3: Joint Intelligence Preparation of the Operational Environment. Washington, DC: Joint Chiefs of Staff. https://irp.fas.org/doddir/military/jp2_01_3.pdf

[19] Joint Chiefs of Staff. 2018. Joint Publication 3-12: Cyberspace Operations. Washington, DC: Joint Chiefs of Staff. https://irp.fas.org/doddir/dod/jp3_12.pdf

[20] Joint Chiefs of Staff. 2022. Joint Publication 3-12: Cyberspace Operations. Rev. ed. Washington, DC: Joint Chiefs of Staff. https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2018-JP-3-12-Cyberspace-Operations.pdf

[21] Lü, G., L. Yuan, and Z. Yu. 2021. "Information Geography: A New Fulcrum of Geographic Ternary World." Science China Earth Sciences 65 (2): 383–386. https://doi.org/10.1007/s11430-021-9859-9

[22] Mills, J. R. 2012. "The Key Terrain of Cyber." Georgetown Journal of International Affairs, special issue: 99-107.

[23] NATO Standardization Office. 2020. AJP-3.20: Allied Joint Doctrine for Cyberspace Operations. Edition A, Version 1. Brussels: NATO Standardization Office. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

[24] UK Ministry of Defence. 2018. Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities. Shrivenham, UK: Development, Concepts and Doctrine Centre. https://assets.publishing.service.gov.uk/media/5a8d6373e5274a5e67567dff/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf

[25] Pingel, T. J. 2003. "Key Defensive Terrain in Cyberspace: A Geographic Perspective." In Proceedings of the International Conference on Politics and Information Systems, 159–163. Orlando.

[26] Price, P., N. A. Leyba, M. Gondree, Z. Staples, and T. Parker. 2017. "Asset Criticality in Mission Reconfigurable Cyber Systems and Its Contribution to Key Terrain Identification." In Proceedings of the 50th Hawaii International Conference on System Sciences. Hawaii. https://doi.org/10.24251/HICSS.2017.729

[27] Raymond, D., G. Conti, T. Cross, and R. Fanelli. 2013. "A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons." In 2013 5th International Conference on Cyber Conflict, 1–16. Tallinn, Estonia: IEEE. https://ccdcoe.org/uploads/2018/10/8_d1r2s6_raymond.pdf

[28] Raymond, D., G. Conti, T. Cross, and M. Nowatkowski. 2014. "Key Terrain in Cyberspace: Seeking the High Ground." In 6th International Conference on Cyber Conflict, edited by P. Brangetto, M. Maybaum, and J. Stinissen, 287–300. Tallinn: NATO CCD COE Publications. https://ccdcoe.org/uploads/2018/10/d2r1s8_raymondcross.pdf

[29] Thomas, T. L. 2004. "Russia's Reflexive Control Theory and the Military." Journal of Slavic Military Studies 17 (2): 237–256. https://doi.org/10.1080/13518040490450529

[30] U.S. Army War College. 2023. Strategic Cyberspace Operations Primer. Carlisle, PA: U.S. Army War College. https://csl.armywarcollege.edu/pubs/Publications/Strategic_Cyberspace_Operations_Primer-2023_Dec_18.pdf

[31] U.S. Department of Defense. 2023. 2023 DoD Cyber Strategy. Washington, DC: U.S. Department of Defense. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf

[32] Venables, A. 2021. "Modelling Cyberspace to Determine Cybersecurity Training Requirements." Frontiers in Education 6: 768037. https://doi.org/10.3389/feduc.2021.768037

[33] Xu, R., Z. Zhang, Z. Rao, J. Chen, M. Li, F. Liu, and S. Pan. 2019. "Cyberspace Surveying and Mapping: Hierarchical Model and Resource Formalization." In IEEE INFOCOM 2019, 68–72. IEEE. https://doi.org/10.1109/INFCOMW.2019.8845226

[34] Ye Zheng. 2013. Lectures on Information Operations (in Chinese). China Academy of Military Science (AMS), Beijing: Military Science Press, 2013

[35] Youn, J., H. Oh, J. Kang, and D. Shin. 2021. "Research on Cyber IPB Visualization Method Based on BGP Archive Data for Cyber Situation Awareness." KSII Transactions on Internet and Information Systems 15 (2): 749–766. https://doi.org/10.3837/tiis.2021.02.020