Operationalizing Cyber in Multi-domain Operations: A Kill-Chain-Centric Approach for Cyber Strike Packages

Timothy Shives, William Stegner, Elizabeth Pham and Lieuwe Jan Hiemstra
Naval Postgraduate School, Monterey, California, USA

timothy.shives@nps.edu
lieuwejan.hiemstra.ne@nps.edu
william.stegner@nps.edu
elizabeth.pham@nps.edu

Abstract: This paper examines the challenge of integrating cyber capabilities into NATO Multi-Domain Operations (MDO) at the operational level. While doctrine emphasizes convergence across domains, cyber is not consistently incorporated into execution processes, particularly within the joint targeting cycle. Drawing on a NATO-aligned instructional vignette and student planning exercises, this study proposes a kill-chain-centric framework using Cyber Strike Packages (CSPs) to synchronize cyber effects with other domains. Observations from the instructional environment indicate that cyber capabilities are frequently underutilized or misaligned with operational timelines when planners lack a structured integration framework. Application of the CSP model improved alignment between cyber effects, targeting decisions, and cross-domain coordination. The findings suggest that cyber integration is primarily a problem of structure and timing rather than capability alone. In particular, planners struggled to align cyber preparation timelines with rapid operational decision cycles. The proposed framework addresses this challenge by organizing cyber effects around target, timing, effect, and assessment within the kill chain. The paper concludes that improving cyber integration in NATO operations does not require entirely new doctrine, but more effective incorporation of cyber into targeting processes, planning timelines, and operational decision-making.

Keywords*:* Multi-domain operations (MDO), Cyberspace operations, Cyber strike packages (CSP), Kill chain, NATO, Joint targeting

1. Introduction

The emerging phenomenon of Multi-Domain Operations (MDO) reflects an ongoing shift in how military power is applied across land, maritime, air, space, and cyberspace, with convergence at its center—the ability to synchronize and orchestrate capabilities across domains to create compounded operational effects and decision advantage (NATO Standardization Office, 2020; Department of Defense, 2022). While this idea is well established in doctrine, its practical implementation, particularly with respect to cyber, remains unclear. Cyber capabilities are often acknowledged as important but are not consistently integrated into execution-level processes, instead being treated as pre-operational shaping tools or specialized activities managed outside the main planning and targeting workflows (Joint Chiefs of Staff, 2022; Libicki, 2021). This creates a gap between what cyber is expected to contribute and how it is actually employed. This is most visible in time-sensitive scenarios where planners demonstrate a general understanding of cyber capabilities but struggle with determining what effect is required, when that effect must occur, and how cyber compares to other available options. This reflects a broader issue identified in doctrine and scholarship. Cyber Persistence Theory and related scholarship on political warfare emphasize continuous engagement, competition below armed conflict, and the strategic use of cyber capabilities to shape adversary behavior (Fischerkeller, Goldman and Harknett, 2022; Jensen, 2022). Where strategic frameworks such as Cyber Persistence Theory emphasize continuous engagement and initiative in cyberspace, these frameworks do not fully translate into operational planning constructs (Fischerkeller, Goldman and Harknett, 2022).

Doctrinal publications, such as AJP-3.20 and JP 3-12, that provide guidance on organizing and employing cyber forces are limited in describing how cyber effects are integrated into joint targeting cycles and kill chain execution (NATO Standardization Office, 2020; Joint Chiefs of Staff, 2022). Scholars have noted this disconnect, highlighting a persistent gap between cyber planning and traditional operational planning processes and the difficulty of aligning cyber effects with operational timelines and decision cycles (VanDriel, 2015; Lindsay, 2020; Libicki, 2021). This results in cyber planning occurring in parallel rather than within operational planning and limiting its impact during execution (VanDriel, 2015; Lindsay, 2020; Libicki, 2021).

This paper examines that problem from an applied perspective, focusing on how cyber capabilities are incorporated into operational planning and decision-making, and proposes a kill-chain-centric approach to cyber integration operationalized through Cyber Strike Packages (CSPs) as a practical method for aligning cyber

capabilities with the structure of the kill chain, the timing of operational decision-making, and the processes used in joint targeting and execution.

The analysis is grounded in a NATO-aligned instructional vignette in which students developed operational plans for a multi-domain scenario, showing that the primary limitation is not technological but procedural and cognitive, and that integration through a kill-chain-centric framework makes cyber a more usable and effective component of multi-domain operations, as has been established in recent real world operations. Despite significant doctrinal development in cyberspace operations, a persistent operational gap remains between recognizing cyber as a critical domain and integrating cyber effects into execution-level planning and targeting. Existing doctrine explains why cyber matters, but provides limited practical guidance for how planners should synchronize cyber capabilities with operational timelines and kill chain execution in Multi-Domain Operations. This paper addresses that gap by proposing a usable planning framework designed to operationalize cyber integration within existing NATO operational structures.

2. Literature and Doctrine Review

Over the past decade, both NATO and U.S. doctrine have made substantial progress in recognizing cyberspace as a distinct warfighting domain. At the same time, a consistent gap remains between conceptual acknowledgment and operational integration. This section reviews the doctrinal and scholarly landscape with a focus on where cyber integration breaks down in practice, particularly within the context of MDO. Existing strategic cyber theories provide important insight into competition and persistent engagement in cyberspace. Their strength lies in explaining how states maintain initiative and strategic advantage through continuous interaction. However, their limitation is that they provide limited operational guidance for synchronizing cyber effects with targeting processes and time-sensitive execution requirements in MDO environments.

2.1 NATO Multi-Domain Operations and the Problem of Execution

NATO's approach to MDO emphasizes the orchestration of military and synchronization of non-military capabilities across domains and environments to create converging effects and achieve operational advantage." (NATO Allied Command Transformation, 2023, NATO Standardization Office, 2020). Allied doctrine, including AJP-3.20: Allied Joint Doctrine for Cyberspace Operations and AJP-6: Communication and Information Systems, establishes cyberspace as both an operational domain and a critical enabler of joint operations. However, while these publications clearly articulate the importance of cyberspace, they provide less detail on how cyber capabilities are incorporated into execution-level processes, particularly within the joint targeting cycle. In practice, cyber is often framed in one of three ways:

- As a supporting function for intelligence or information activities,
- As a pre-operational shaping tool, or
- As a strategic-level instrument of competition.

What is less clearly defined is how cyber contributes to time-sensitive targeting. From a planning perspective, this creates friction. Planners understand that cyber is important, but they often lack a clear method for incorporating it into courses of action, weaponeering, and execution timelines. This challenge is amplified in coalition environments, where authorities, capabilities, and information-sharing constraints vary by nation. As a result, cyber may be conceptually integrated into NATO MDO, but remains uneven in execution.

2.2 Persistence Without Operationalization

At the strategic level, one of the most influential contributions to cyber theory is Cyber Persistence Theory, which introduces the concept of persistent engagement, arguing that cyberspace is characterized by continuous interaction among adversaries where advantage is gained through initiative and sustained activity rather than discrete campaigns (Fischerkeller, Goldman and Harknett, 2022). However, from an operational standpoint, the theory does not fully address how these dynamics translate into time-bound, synchronized effects within military operations, nor does it provide a clear framework for integrating cyber into joint targeting processes, aligning cyber effects with operational timelines, or incorporating cyber into kill chain execution. U.S. joint doctrine, particularly Joint Publication 3-12: Cyberspace Operations, provides more detailed guidance on the organization and execution of cyber operations (Joint Chiefs of Staff, 2022), emphasizing integration with the Joint Planning Process and the joint targeting cycle, and outlining the roles of Offensive Cyber Operations (OCO) and Defensive Cyber Operations (ISR).

Despite this, a planning gap remains. Cyber planning often occurs in parallel to operational planning rather than within it (VanDriel, 2015), leading to recurring issues in which cyber capabilities are introduced late in the planning process, cyber effects are not aligned with key decision points, and non-cyber planners lack confidence in how to employ cyber options. More recent scholarship reinforces this observation, noting that cyber operations are difficult to integrate due to their dependence on access, intelligence, uncertain effects, and escalation dynamics (Lindsay, 2020; Libicki, 2021; Borghard and Lonergan, 2021). This highlights the challenge of aligning cyber capabilities with operational objectives, particularly when outcomes are indirect or difficult to measure (Libicki, 2021). This results in cyber being frequently underutilized or misapplied even when available.

2.3 Cyber Effects in Operational Context

A related challenge concerns the nature of cyber effects themselves. Cyber effects are often difficult to attribute, uncertain in duration, and challenging to employ for traditional deterrence purposes (Nye, 2017). Unlike kinetic effects, which are typically observable and immediate, cyber effects can be delayed or time-dependent, reversible or temporary, difficult to attribute, and dependent on sustained access. These characteristics complicate integration into traditional planning models. As Rid (2020) and Valeriano and Maness (2018) argue, cyber operations are often more effective as disruption and shaping tools rather than decisive, standalone actions. This does not diminish their operational value, but it does require a different approach. Cyber must be aligned with other domain effects to produce meaningful outcomes. In practice, however, this alignment is difficult to achieve without a structured framework.

2.4 Synthesis: The Missing Operational Framework

Taken together, doctrine and scholarship point to consistent conclusions:

- Strategic understanding of cyber is well developed,
- Capabilities continue to evolve, and
- Doctrine recognizes cyberspace as essential.

However, a gap remains at the operational level, particularly in integrating cyber into the kill chain, synchronizing cyber with targeting processes, and aligning cyber effects with operational timelines. This gap is not simply theoretical—it directly affects how operations are planned and executed. Without a practical framework, cyber remains conceptually important and technically capable, but operationally underutilized.

3. Conceptual Framework: Kill-Chain-Centric Cyber Integration

The preceding section highlighted a consistent gap between how cyber is discussed in doctrine and how it is actually used during planning and execution. This section introduces a kill-chain-centric framework, supported by the concept of Cyber Strike Packages (CSPs), as a means to address that gap.

3.1 Reframing the Kill Chain in a Multi-domain Context: Cyber Strike Package (CSP)

The evolution towards “kill chain centric operations” as a fundamental warfighting concept is being explored in naval combat (Stegner, 2026). There is a natural extension of this thinking into cyber operations. The kill chain—commonly described as *find, fix, track, target, engage, and assess*—is a foundational construct for organizing military effects and has increasingly been applied across domains as a way to structure decision-making and synchronize capabilities (Joint Chiefs of Staff, 2022). Cyber is rarely mapped explicitly to kill chain phases and is often treated as a prerequisite activity (e.g., access development), an intelligence enabler (e.g., support Intelligence, Surveillance and Reconnaissance), or a standalone effect delivered independently of broader operations, creating a disconnect that makes it difficult for planners to determine where cyber can have the greatest operational impact, when effects must occur, and how cyber aligns with other domain actions. To address this, the proposed framework maps cyber contributions directly to each phase of the kill chain:

Kill Chain Phase	Cyber Contribution
Find / Fix	Network reconnaissance, target identification
Track	Persistent access, telemetry collection
Target	Vulnerability analysis, access validation
Engage	Effects delivery (disrupt, deny, manipulate, destroy)
Assess	Cyber-enabled battle damage assessment

Figure 1: Kill-Chain-Centric Cyber Integration

This provides a common reference point for integrating cyber into operational planning discussions. This conceptual mapping is operationalized through Cyber Strike Packages (CSPs), defined as "a coordinated set of cyber actions designed to achieve a specific operational effect within a defined time window, aligned with the joint targeting process," structured to resemble traditional strike packages used in air and fires planning. Each CSP includes five core elements:

- Target definition—the system, network, or function to be affected, linked to an operational objective;
- Access and placement—the method and level of access required, including persistence and reliability;
- Effect type—the intended outcome (e.g., disruption, denial, manipulation, destruction);
- Timing and execution window—when the effect must occur relative to decision points and other domain actions;
- Assessment mechanism—how success will be measured, including both performance and effectiveness.

3.2 Red and Blue Kill Chain Interaction

A key advantage of integrating cyber into the kill chain framework is that it allows planners to consider both friendly and adversary processes simultaneously. In a multi-domain environment, operations involve the interaction of the adversary (Red) kill chain, and the friendly (Blue) kill chain. Cyber is uniquely positioned to influence both. From an adversary-focused perspective, cyber can disrupt detection and tracking systems, degrade communications between nodes, and delay or prevent engagement decisions. From a friendly perspective, cyber can enable targeting through improved intelligence, provide access to critical information, and support synchronization across domains. From a multi-domain operations perspective, cyber capabilities can be viewed as "shoot to move" and "move to shoot" that integrates with the concepts of fire and maneuver that directly translate into risk to mission and risk to force. In some cases, effective employment of cyber capabilities can reduce both risk to mission and risk to force at the same time.

3.3 Effects-based Thinking in Cyber Planning

One of the most consistent challenges observed in planning environments is the tendency to focus on capability rather than effect. This aligns with broader observations in literature, where cyber discussions often emphasize technical feasibility over operational impact (Lindsay, 2020; Libicki, 2021). The kill-chain-centric approach shifts the focus toward effects-based thinking, which is already well established in targeting doctrine. This requires planners to begin with questions such as:

- What operational outcome is required?
- How does this engagement support fire and maneuver in other domains?
- What effect will produce that outcome?
- Which capability is best suited to deliver it?

3.4 Temporal Dynamics and Synchronization

The most significant challenge in integrating cyber into the kill chain is time. Cyber operations often involve extended preparation periods for access development, uncertain execution timelines, and variable effect duration. These characteristics contrast with the compressed timelines of modern operations. The Cyber Strike Package (CSP) framework addresses this by explicitly incorporating preparation time ("walk-time"), execution windows, and duration of effect. This forces planners to treat cyber as a time-dependent capability, rather than something that can be applied on demand.

3.5 The Role of the Planner

Integrating cyber into the kill chain ultimately depends on how planners approach the problem. This requires a functional understanding of cyber capabilities, the ability to incorporate cyber into existing processes (e.g., targeting), and coordination across domains and organizations. This would represent a shift in mindset. Cyber should no longer be treated as a specialized activity managed separately, but as part of how operations are designed and executed. The kill-chain-centric framework and the Cyber Strike Package (CSP) construct provide a way to conceptualize and plan cyber integration.

4. Operational Integration: The NATO Joint Operations Centre (JOC)

Within NATO operational structures, responsibility for conceptualizing and planning cyber integration sits with the Joint Force Command (JFC) and, more specifically, the Joint Operations Centre (JOC), where planning outputs are translated into synchronized execution. Within NATO command structures, the JOC functions as the central node for monitoring ongoing operations, synchronizing joint effects across components, and supporting commander decision-making through a structured battle rhythm that links planning, targeting, execution, and assessment, becoming the point where convergence either happens or breaks down in a MDO context.

While NATO doctrine emphasizes coordination across domains and the importance of integrated command and control (NATO Standardization Office, 2019; 2020), it provides less detail on how cyber capabilities are incorporated into execution-level processes, particularly those tied to the joint targeting cycle. This creates a challenge in which planners understand that cyber should be included but lack clarity on where and how it fits into the workflow. Cyber is often positioned outside the main execution cycle because capabilities are managed through specialized organizations or reach-back elements, where authorities remain at the national level, and information is constrained by classification or policy (SCEPVA), resulting in cyber planning occurring in parallel to operational planning rather than within it (VanDriel, 2015; Lindsay, 2020). This leads to recurring issues in which cyber options are not consistently presented during targeting discussions, cyber effects are not aligned with operational decision timelines, and planners lack confidence in how cyber can be employed.

The Cyber Strike Package (CSP) framework provides a way to integrate cyber into existing JOC processes without requiring significant structural changes by aligning cyber with already existing planning and execution, by incorporating cyber into mission analysis, course-of-action development and analysis, and the joint targeting cycle. Convergence becomes executable through target development, capability selection, and execution planning. This allows cyber to be evaluated alongside other capabilities in terms of expected effect, timing, duration, escalation risk, and attribution considerations (Borghard and Lonergan, 2021).

Effective integration requires intelligence support and continuous feedback loops between intelligence and operations for identifying target systems, validating access, and assessing effects (Rid, 2020; Valeriano and Maness, 2018). The same applies for visibility within the JOC battle rhythm, including targeting boards, operations updates, and commander briefs, where cyber options must be presented, aligned with decision timelines, and incorporated into operational assessments. When these conditions are met, the JOC functions as a convergence engine, synchronizing effects across domains, enabling coordinated action, and increasing operational tempo and complexity.

NATO operations introduce additional complexity through coalition dynamics, including national caveats, capability asymmetry, and information-sharing constraints, particularly for sensitive capabilities (Libicki, 2021). The Cyber Strike Package (CSP) framework helps mitigate these issues by focusing on effects rather than capabilities, allowing coordination without requiring full visibility into execution. This is critical, since the overall effectiveness of cyber capabilities depends on how planners apply these concepts to synchronize multi-domain effects in time-constrained operational environments.

5. Operational Application: NATO MDO Instructional Vignette

To examine how cyber capabilities can be incorporated into MDO in practice, this study draws on a NATO-aligned instructional vignette used in an instructor-level course. The vignette provides a structured, time-constrained environment in which students are required to develop operational plans that integrate capabilities across domains. Rather than relying on retrospective case studies, this approach allows for direct observation of how planners think, where integration breaks down, and what changes when a structured framework is introduced. It also captures decision-making under conditions that approximate operational pressure, including limited time, incomplete information, and competing priorities.

5.1 Scenario Overview and Operational Context

The vignette centers on a maritime scenario in which NATO forces are tasked to impose sea denial in the vicinity of a fictional city in a fictional country in order to isolate adversary forces. The operational problem is defined through a set of tactical tasks, including the attrition on the adversary's maritime capability, and degrading coastal defense systems. A defining feature of the scenario is the characterization of the adversary's kill chain as operating on a six-minute timeline from detection to weapon release. The following is a graphical depiction of the vignette that has been edited with artificial intelligence to change the location for publication purposes.

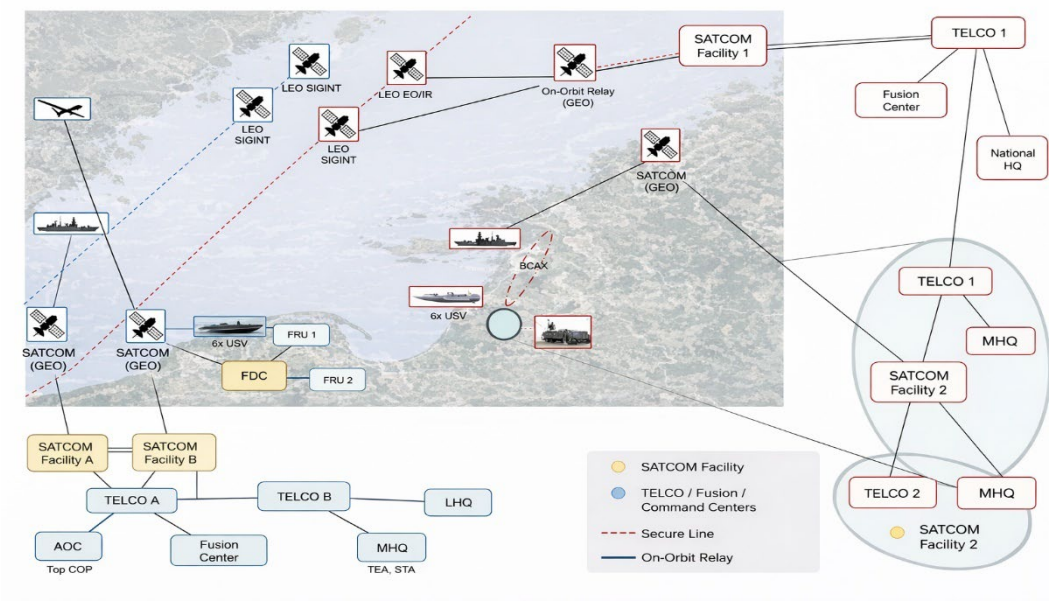

Figure 2: Operational Vignette depicting Command and Control (C2) Architecture

From the outset, this creates a clear tension as the adversary operates on a minutes-based timeline, and where in contrast, many cyber effects require hours—or longer—of preparation beyond their development and requirements for gaining access. In practice, this tension became one of the central planning challenges. Students quickly recognized that cyber could be useful but questioned whether those effects could be delivered in time to influence the outcome.

5.2 System Architecture and Target Environment

The vignette includes a detailed representation of the adversary's command-and-control architecture. This consists of national and maritime headquarters nodes, fusion centers responsible for data aggregation and decision support, telecommunications (TELCO) infrastructure, and satellite communications (SATCOM) facilities and on-orbit relay systems.

This architecture reflects a distributed, network-dependent system, where operational effectiveness depends on the ability to move information across multiple nodes. The target list reinforces this structure, identifying key systems such as the Maritime Headquarters (MHQ), Fusion Centers, TELCO nodes, and SATCOM facilities. Many of these targets are designated for cyber strike consideration, particularly those associated with command and control (C2). This shifts the problem from simply targeting platforms to identifying critical functions within the adversary's kill chain.

5.3 Cyber Strike Packages in the Scenario

To support planning, the vignette provides a set of predefined Cyber Strike Packages (CSPs). These packages include a designated target, an effect type (e.g., disrupt, deny, manipulate), a preparation time ("walk-time"),

an expected duration of effect, and considerations such as attribution and reversibility. For example, disrupting a headquarters node may require longer preparation but produce sustained effects, manipulating a fusion center may be faster but shorter in duration and denying TELCO infrastructure may produce immediate impact but carry greater escalation risk. These Cyber Strike Packages (CSPs) introduce trade-offs that planners must evaluate, including speed versus persistence, reversibility versus decisiveness, and operational impact versus attribution risk.

6. Analysis: Wargaming Insights

The instructional vignette provides a controlled environment to examine how cyber capabilities are incorporated into operational planning. By comparing planning behavior before and after the introduction of the kill-chain-centric Cyber Strike Package (CSP) framework, several patterns emerge. These patterns help explain why cyber remains underutilized in practice and what changes when a structured approach is applied.

6.1 Baseline Condition: Cyber Without a Structured Framework

Across early planning iterations, cyber integration was inconsistent and often superficial, not due to a lack of awareness, but due to difficulty translating that understanding into operationally relevant decisions. Cyber was frequently separated from the main planning effort and not fully incorporated into course-of-action development, targeting decisions, or execution timelines. Instead, it appeared as an add-on that could be included if time allowed, as reflected in the literature (VanDriel, 2015; Lindsay, 2020).

Most groups defaulted to kinetic solutions, particularly against maritime targets, favoring capabilities with more predictable and immediate outcomes (Lindsay, 2020), while cyber was treated as a supporting function for intelligence collection or general disruption rather than as a targeted tool for influencing specific points in the adversary's kill chain. A related issue was the tendency to focus on capability (options) rather than effect, resulting in cyber being underutilized or misaligned with operational objectives. Timing further compounded these challenges, as cyber options were selected without fully accounting for preparation time, execution windows, or alignment with key decision points, leading to effects that would occur after the critical operational moment and limiting their usefulness.

6.2 Temporal Misalignment as a Primary Constraint

A consistent takeaway is that cyber integration is fundamentally a timing and synchronization problem, as students generally understood what cyber could do but struggled to determine whether those effects could be delivered in time and aligned with the pace of operations. Across nearly all groups, timing emerged as the primary constraint on effective cyber integration, with cyber effects identified as operationally relevant but difficult to align with required timelines, particularly in relation to the adversary's six-minute kill chain. Cyber actions were often planned too late, preparation time was not accounted for, and effects occurred after the critical decision point had passed, highlighting that effects requiring hours of preparation could still be effective only if planned and initiated early enough. This aligns with findings in the literature that cyber operations are difficult to synchronize due to their dependence on access and preparation (Lindsay, 2020; Libicki, 2021) but also indicates that the problem is not purely technical, as planners were not consistently incorporating cyber timelines into early planning. The Cyber Strike Package (CSP) framework helped address this by requiring planners to account for preparation time, align execution with decision points, and treat cyber as a time-dependent capability rather than an on-demand option.

6.3 Effects-Based Framing and Its Impact on Planning

When the Cyber Strike Package (CSP) framework was introduced and explicitly tied to the kill chain, planning behavior began to shift toward effects-based thinking. Instead of starting with available capabilities, students were required to define the desired operational effect, the point in the kill chain where that effect would have the greatest impact, and the timing required to achieve it.

This shift had several observable effects. First, cyber was introduced earlier in the planning process. Second, cyber effects became more specific. Third, cyber was more consistently integrated into targeting discussions. When presented in CSP format, cyber could be evaluated alongside kinetic and electronic warfare options, making it easier for planners to incorporate it into decision-making.

6.4 Kill Chain Disruption as an Organizing Logic

When the kill-chain-centric Cyber Strike Package (CSP) framework was applied, planning behavior began to change, particularly in how targets were conceptualized, shifting from platform-centric targets towards alignment with specific phases of the kill chain, enabling disruption of tracking systems, degradation of communication between nodes, and delays in decision-making processes, resulting in more deliberate and targeted use of cyber capabilities. This reflects a broader shift in multi-domain thinking, where the objective is not simply to destroy platforms, but to disrupt the underlying processes (Department of Defense, 2022), with cyber proving particularly effective in this role by delaying detection, degrading tracking accuracy, and disrupting coordination between nodes. Integration across domains also improved, as cyber effects were increasingly

synchronized with maritime fires, ISR collection, and electronic warfare activities, and in some cases combined with kinetic effects to degrade adversary awareness while positioning assets for follow-on action.

6.5 Persistent Friction Points

Improvements in cyber integration were not uniform across all groups, as under time pressure some teams reverted to kinetic-first planning even when cyber options were available, indicating that frameworks such as Cyber Strike Package (CSPs) improve integration but do not fully overcome familiarity with traditional capabilities, uncertainty associated with cyber effects, or cognitive biases in decision-making. Coalition dynamics also remained a complicating factor, as not all partners possess the same capabilities and some cyber effects are constrained by national authorities, adding complexity to planning. These observations highlight the importance of repetition and reinforcement, as integration improved over time but required multiple iterations and guided discussion, demonstrating that cyber integration challenges emerge during planning and can be partially addressed through structured frameworks.

6.6 Cyber Integration

When properly integrated, cyber can disrupt adversary decision-making timelines, create opportunities for other domains, and increase the tempo and complexity of operations. However, this potential is only realized when cyber is aligned with the kill chain, integrated into targeting processes, and synchronized with operational timelines. Specifically, effective cyber integration can be achieved by:

- A Common Framework: The kill chain provides a shared structure for organizing cyber effects.
- A Practical Planning Construct: Cyber Strike Packages (CSPs) translate conceptual integration into actionable planning.
- Process Integration: Cyber must be incorporated into targeting and execution processes.
- Temporal Alignment: Cyber timelines must be considered early in planning, not after the fact.

The outcomes observed in the instructional environment support the argument that cyber integration improves when planners are provided with structured methods that align cyber effects with operational decision cycles. The observed improvements in synchronization, targeting integration, and effects-based planning justify the use of CSPs as a practical operational construct rather than solely a conceptual framework.

7. Implications for NATO Doctrine, Planning, and Training

The analysis suggests that the central challenge in integrating cyber into Multi-Domain Operations (MDO) is not a lack of capability, but a gap in how those capabilities are incorporated into operational processes. NATO doctrine recognizes cyberspace as a critical domain and emphasizes convergence and the integration of capabilities across domains (NATO Standardization Office, 2020). This challenge is increasingly important in environments characterized by persistent competition and political warfare below the threshold of conventional conflict (Jensen, 2022). However, the translation of that recognition into execution-level integration remains unclear, as cyber is often acknowledged during planning but not consistently incorporated into targeting decisions, execution timelines, or commander decision cycles. Bridging this gap requires more than doctrinal recognition. Thus, this requires clearer linkage between cyber and execution processes and planning constructs that allow cyber to be incorporated without requiring deep technical expertise, highlighting that usability, not just availability, is a key factor in integration.

7.1 Integrating Cyber into the Joint Targeting Cycle

The joint targeting cycle remains the primary mechanism through which convergence is achieved in practice. Despite this, cyber is not always fully integrated into target nomination, capability selection, or effects synchronization. The Cyber Strike Package (CSP) framework suggests a way to address this gap. By structuring cyber options in terms of target, effect, timing, and risk, cyber can be evaluated alongside kinetic and electronic warfare options. In the instructional environment, once cyber options were presented in this format, they were more consistently included in targeting discussions. This did not require new capabilities, only a different way of presenting them. The implication is that NATO may benefit from further developing methods that allow cyber to be consistently represented within targeting processes, particularly at the operational level.

7.2 Addressing Temporal Mismatch

One of the most consistent findings in this study is the impact of temporal mismatch on cyber integration.

Cyber operations often require preparation time for access development, and coordination with intelligence and supporting elements. These timing challenges complicate traditional concepts of deterrence and response in cyberspace, particularly when operational decision cycles occur faster than cyber preparation timelines (Nye, 2017). Cyber timelines need to be incorporated into planning from the outset. Planning processes should more explicitly account for the temporal characteristics of cyber operations, particularly during early stages of course-of-action development.

7.3 Coalition Considerations

Cyber integration in NATO operations is further complicated by coalition dynamics. These include national caveats and authorities, uneven distribution of cyber capabilities, and constraints on information sharing.

These challenges are well documented and are unlikely to be resolved through doctrine alone (Libicki, 2021). However, the findings suggest that how cyber is framed can influence how it is integrated. By focusing on effects rather than capabilities, the Cyber Strike Package (CSP) framework allowed planners to coordinate cyber actions without requiring full visibility into how those actions would be executed. In practice, this approach made integration more feasible in a simulated coalition environment. Students were able to coordinate cyber effects conceptually, even when detailed technical information was limited. The implications are that effects-based approaches may help mitigate some of the practical challenges associated with coalition cyber operations, particularly where full transparency is not possible.

7.4 Training and Education

The vignette highlights that cyber integration is not only a doctrinal issue, but also a training and education challenge. Several patterns were observed: (1) planners defaulted to kinetic options in early iterations, (2) cyber was underutilized without structured guidance, and (3) integration improved with repetition and feedback. These observations suggest that effective integration requires familiarity with cyber as a planning tool, practice applying cyber in operational contexts, and reinforcement of effects-based thinking. The implication is that professional military education and training programs may benefit from incorporating structured cyber planning constructs and scenario-based exercises that emphasize timing, targeting, and cross-domain integration.

7.5 Toward a More Usable Operational Approach

The findings suggest that improving cyber integration does not necessarily require entirely new doctrine. Referencing the previous section (6.6) instead, the new conceptual framework may involve refining how existing concepts are applied in practice. Key elements of a more usable approach include:

- Mapping cyber effects to the kill chain,
- Incorporating cyber into the targeting cycle,
- Accounting for timing constraints, and
- Using planning constructs accessible to non-specialists.

The Cyber Strike Package (CSP) framework represents one way to bring these elements together. It is not intended as a definitive solution, but as a practical tool that aligns cyber with how operations are already planned and executed.

8. Conclusion

This paper examined the challenge of integrating cyber capabilities into NATO Multi-Domain Operations at the operational level. Although cyberspace is recognized as a critical domain, cyber effects remain inconsistently integrated into execution-level planning and targeting processes. Using a NATO-aligned instructional vignette, this study demonstrated that planners often struggle to synchronize cyber effects with operational timelines, particularly in time-sensitive environments. The findings suggest that the primary obstacle is not capability, but the absence of practical planning constructs that align cyber with kill chain execution and operational decision-making. The proposed kill-chain-centric framework and Cyber Strike Packages (CSPs) provide a usable method for incorporating cyber into targeting, synchronization, and cross-domain planning. Application of this framework improved integration of cyber effects within operational planning and increased alignment between cyber and other domain capabilities. Future research should examine how artificial intelligence-assisted planning tools, automated targeting support, and coalition information-sharing mechanisms may further improve synchronization of cyber effects in Multi-Domain Operations (MDO). Additional research should examine the framework within larger-scale exercises, coalition environments, and quantitative assessments of

operational effectiveness. As NATO continues refining MDO concepts, cyber must be integrated not as a separate supporting activity, but as part of operational execution itself.

9. Abbreviations

The following is a reference list of abbreviations used in throughout this article.

Abbreviation	Meaning
C2	Command and Control
CSP	Cyber Strike Package
DCO	Defensive Cyber Operations
ISR	Intelligence, Surveillance, and Reconnaissance
JFC	Joint Force Command
JOC	Joint Operations Centre
MDO	Multi-Domain Operations
MHQ	Maritime Headquarters
NATO	North Atlantic Treaty Organization
OCO	Offensive Cyber Operations
SATCOM	Satellite Communications
TELCO	Telecommunications

Figure 3: Kill-Chain-Centric Cyber Integration

Ethics Declaration: Ethical clearance was not required for this research.

AI Declaration: Open-source artificial intelligence (AI) tools were used solely for proofreading and citation formatting. All analysis, arguments, and conclusions presented in this paper are the original work of the authors or are derived from appropriately cited sources. Finally, the operational vignette in Figure 2 was edited with AI in order to generalize the scenario for publication purposes.

Disclaimer: The views expressed here are those of the authors and do not necessarily represent the views of the Naval Postgraduate School, the Department of War, or the U.S. Government.

References

Borghard, E.D. and Lonergan, S.W., 2021. Cyber operations as imperfect tools of escalation. *International Security*, 45(3), pp.55–102.

Borghard, E.D. and Lonergan, S.W., 2021. The logic of coercion in cyberspace. *Security Studies*, 30(3), pp.335–366.

Department of Defense, 2022. *2022 National Defense Strategy of the United States of America*. Washington, DC: U.S. Department of Defense.

Fischerkeller, M.P., Goldman, E.O. and Harknett, R.J., 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace*. Oxford: Oxford University Press.

Harknett, R.J. and Goldman, E.O., 2022. Cyber persistence and strategic competition. *Journal of Cybersecurity*, 8(1), pp.1–15.

Jensen, B., 2022. *The Cyber Character of Political Warfare*. Oxford: Oxford University Press.

Joint Chiefs of Staff, 2022. *Joint Publication 3-12: Cyberspace Operations*. Washington, DC: Department of Defense.

Libicki, M.C., 2021. *Cyberspace in Peace and War*. Annapolis, MD: Naval Institute Press.

Lindsay, J.R., 2020. *Information Technology and Military Power*. Ithaca, NY: Cornell University Press.

NATO Allied Command Transformation, 2023. *Multi-Domain Operations Concept*. Norfolk, VA: NATO ACT.

NATO Standardization Office (NSO), 2019. *Allied Joint Doctrine for Communication and Information Systems (AJP-6)*. Brussels: NATO.

NATO Standardization Office (NSO), 2020. *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20)*. Brussels: NATO.

Nye, J.S., 2017. Deterrence and dissuasion in cyberspace. *International Security*, 41(3), pp.44–71.

Rid, T., 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.

Stegner, W., 2026. The Great Paradigm Shift of our time: Kill Chain Centric Operations - The Fundamental Warfighting Concept for Next Generation Naval Combat, *Naval War College Review*, [Unpublished manuscript].

Valeriano, B. and Maness, R.C., 2018. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press.

VanDriel, E., 2015. Bridging the planning gap: Incorporating cyberspace into operational planning. *Small Wars Journal*. Available at: https://smallwarsjournal.com (Accessed: 24 March 2026).