Jurnal Peperangan Asimetris
Volume 12, Nomor 1 2026 E-ISSN 2830-0475

Cyber to Blind, Kinetic to Break: Bounding Cyber-Enabled Operations in Cross-Domain Kill Chains

Cyber to Blind, Kinetic to Break: Menetapkan Batas Operasi Berbasis Siber dalam Rantai Pembunuhan Lintas Domain (Cross-Domain Kill Chains)

Yashwant

Fakultas Strategi Pertahanan Darat, UNHAN RI
(yashccmail@gmail.com)

Abstract
While cyberspace is increasingly recognized as a distinct military domain, empirical examples of cyber capabilities directly triggering decisive kinetic outcomes remain historically rare. This article conceptualizes and defines Cyber-Enabled Kinetic Operations (CEKO) as a unique operational category of warfare where cyberspace activities are deliberately leveraged to plan, support, or execute traditional lethal, physical military strikes. Utilizing a qualitative comparative case study framework and process tracing , the study analyzes four distinct operational theaters: the radar-spoofing campaign in Operation Orchard (2007) , tactical espionage in the Donbas (2014–2016) , the Viasat satellite infrastructure disruption (2022) , and the multi-domain Caracas infrastructure blackout during Operation Absolute Resolve (2026). The comparative findings indicate that true CEKO frameworks depend heavily on intentional cross-domain planning, long-term persistent network access, and tightly synchronized execution timelines. Ultimately, these findings validate that cyber power functions predominantly as an environmental and preparatory enabler rather than an independently decisive strategic weapon. However, when nested within a multi-domain kill chain, CEKO can directly facilitate high-impact physical outcomes in tandem with conventional military force. The article offers a refined set of working criteria to help operationalize these conceptual boundaries for joint military doctrine, tactical targeting laws, and physical defense resilience.

Keywords: Cyber-Enabled Kinetic Operations (CEKO), multi-domain operations, process tracing, strategic studies, military doctrine, cyber warfare.

Abstrak
Meskipun ruang siber semakin diakui sebagai salah satu domain operasi militer yang berdiri sendiri, bukti empiris mengenai kemampuan siber yang secara langsung menghasilkan dampak kinetik yang bersifat menentukan masih relatif jarang ditemukan dalam sejarah konflik modern. Artikel ini mengonseptualisasikan dan mendefinisikan Cyber-Enabled Kinetic Operations (CEKO) sebagai suatu kategori operasi peperangan yang memanfaatkan kapabilitas siber secara sengaja untuk merencanakan, mendukung, atau mengeksekusi serangan militer konvensional yang menghasilkan efek fisik dan mematikan.
Penelitian ini menggunakan pendekatan studi kasus komparatif kualitatif dengan metode process tracing untuk menganalisis empat teater operasi yang berbeda, yaitu: kampanye manipulasi radar dalam Operation Orchard (2007), operasi spionase taktis di kawasan

Donbas (2014–2016), gangguan terhadap infrastruktur satelit Viasat (2022), serta pemadaman infrastruktur multidomain di Caracas dalam Operation Absolute Resolve (2026). Hasil analisis komparatif menunjukkan bahwa kerangka Cyber-Enabled Kinetic Operations (CEKO) yang sesungguhnya sangat bergantung pada perencanaan lintas domain yang disengaja, keberhasilan memperoleh akses jaringan secara persisten dalam jangka panjang, serta sinkronisasi waktu pelaksanaan yang sangat ketat. Temuan penelitian ini menegaskan bahwa kekuatan siber pada dasarnya lebih berfungsi sebagai faktor pendukung (enabler) yang membentuk lingkungan operasi dan mempersiapkan keberhasilan tindakan militer, dibandingkan sebagai senjata strategis yang secara mandiri mampu menghasilkan kemenangan yang menentukan. Namun demikian, apabila diintegrasikan ke dalam rantai pembunuhan lintas domain (cross-domain kill chain), kapabilitas siber dapat secara langsung memfasilitasi tercapainya dampak fisik yang signifikan melalui sinergi dengan kekuatan militer konvensional. Artikel ini menawarkan seperangkat kriteria operasional yang lebih komprehensif untuk memperjelas batas konseptual Cyber-Enabled Kinetic Operations (CEKO) sebagai landasan pengembangan doktrin operasi gabungan, hukum penargetan militer, serta strategi peningkatan ketahanan pertahanan terhadap ancaman fisik.

Kata kunci: Cyber-Enabled Kinetic Operations (CEKO), operasi multidomain, process tracing, studi strategis, doktrin militer, peperangan siber.

1. Introduction

The 21st century's "cyber revolution" promises new ways to influence warfare, yet major-power conflicts have so far seen only limited blending of cyber and kinetic means. Concepts like multi-domain operations and network-centric warfare envision cyberspace as a combat domain on par with land, air, and sea. Militaries publish doctrines treating cyber capabilities both as independent instruments and as shaping tools for conventional forces. Yet academic security scholars warn that cyber "effects" often remain indirect or non-lethal. Despite this caution, some analysts highlight cases where cyber activity did seem directly tied to military objectives. The 2026 Operation Absolute Resolve in Venezuela and Israel's 2007 strike on a Syrian reactor (Operation Orchard) have been cited as instances of cyber power aiding a raid. These observations suggest a need to define and analyze Cyber-Enabled Kinetic Operations – situations where cyber tools are planned and executed specifically to support or enable a physical strike.

This article argues that: CEKO are a distinct operational category requiring both intentional cross-domain planning and demonstrated linkage between cyber actions and kinetic effects. To substantiate this, we review key literature (Section 2), clarify the concept (Section 3), outline our methodology (Section 4), and trace several high-profile case studies (Section 5). We compare cases in a summary table, then offer new theoretical insights (Section 6) and

practical recommendations (Section 7). The primary contribution of this article is conceptual; the empirical cases serve as illustrative tests of the proposed framework rather than as an exhaustive dataset from which to derive general theory. The goal is an academic-quality analysis for security studies audiences, grounded in primary sources and solid evidence.

2. Literature Review

2.1 Conceptual Foundations. Cyber "power" and its integration into warfare have been widely discussed. Rid (2012) argues that what is often called "cyber war" is in fact centuries-old warfare in new dress: cyberattacks essentially serve as sophisticated sabotage, espionage, or subversion. Similarly, Valeriano and Maness (2015) caution that cyber effects are typically coercive or informational, not outright destructive in kinetic terms. By contrast, Kello (2013) and Lindsay (2015) highlight cyber's systemic effects: it is a virtual weapon reshaping power balances. In practice, Erica Borghard et al. (2021) note that Western militaries have begun planning cyber as both an independent force and a shaping tool to "enable conventional operations". For instance, U.S. doctrines emphasize using cyber for reconnaissance, degrading enemy C4I, or targeting data links, analogized to historical airpower tasks. NATO doctrines now classify cyberspace as a full domain alongside land, air, sea, and space, implying joint force commanders must "orchestrate military activities across all domains".

2.2 CEKO vs. Related Concepts. The literature distinguishes cyber operations (attacks, defense, espionage) from cyber's role in information warfare or electronic warfare. CEKO specifically involves cyberspace tools directly facilitating a physical strike. For example, Bonner (2014) describes the 2008 Georgia conflict as a case where "cyber power… was integrated with traditional kinetic military operations," performing tasks like reconnaissance and interdiction to compel enemy mistakes. On the other hand, Libya and Syria conflicts saw many cyber-espionage and propaganda campaigns with no obvious kinetic linkage. Libicki (2020) asks whether cyberspace is being used as a stepping-stone to physical aggression; he concludes that for now cyber typically follows rather than triggers kinetic action. This suggests CEKO should be defined narrowly: not every cyberattack is CEKO, only those where a cyber action is planned as part of the kill chain for a physical operation.

2.3 Doctrinal and Policy Sources. Official doctrines and think-tank analyses add important context. JP 3-12 (U.S. Joint Cyberspace Doctrine) and similar publications stress integration: cyberspace operations must be deconflicted and synchronized with air, land and naval

operations. A U.S. Joint Staff study notes that “cyberspace actions, carefully controlled can enable lethal and nonlethal effects in the physical domains”. Allied analyses likewise warn that failure to coordinate across domains risks squandered potential. Yet military education surveys find gaps: often officers lack a conceptual grasp of cyber’s battlefield role. This report aims to fill that gap by rigorously examining how cyber effects have indeed (or have not) crossed into physical warfare in documented cases.

3. Defining Cyber-Enabled Kinetic Operations

We define Cyber-Enabled Kinetic Operations (CEKO) as operations in which cyberspace capabilities are deliberately leveraged to plan, support, or execute a traditional lethal (or physical) military effect. In other words, cyber activities are not used in isolation but are integrated into an operation where a physical (kinetic) outcome is the primary goal. Concretely, CEKO involve:

- Planned linkage: Cyber tasks are planned from the outset as part of the operation’s scheme of manoeuvre, not incidental sideline actions.
- Access and Exploitation: Adversary networks, sensors, or communications are penetrated (gaining access) and manipulated or harvested (exploitation) to obtain knowledge or create vulnerabilities.
- Kinetic Connection: The intelligence or disruption resulting from cyber tools is used to shape targeting or timing of a physical strike. For example, feeding false radar data or revealing hidden assets.
- Operational Advantage: The combined cyber-physical action yields a clear advantage (e.g. destroying equipment, saving friendly lives) that would not occur absent the cyber component.

This is distinct from independent cyberwar (where damage is done solely by cyber means, like wiping servers) or traditional information warfare (psychological operations, propaganda). CEKO typically assume the existence of a pending kinetic attack or defend against one. They require cross-domain planning and coordination, akin to integrating air strikes with ground assaults. If cyber effects are merely preparatory (e.g. espionage for future decisions) or incidental (occurring outside battle plans), we would not call them CEKO.

We propose these working criteria for CEKO: (1) Intentional Cross-Domain Planning, (2) Targeted Cyber Access to relevant systems, and (3) Clear Causal Link to the kinetic outcome. Satisfying these conditions distinguishes CEKO from unrelated cyber actions. In later analysis (Section 6) we refine these criteria and discuss boundaries (for example, we exclude autonomous drone hacking that causes immediate kinetic action unless it was part of a preplanned military operation).

4. Methodology: Comparative Case Studies and Process Tracing

To analyse CEKO rigorously, we use a qualitative comparative case study approach (cf. George & Bennett 2005). We selected cases where open-source evidence suggests cyber capabilities were intentionally used in conjunction with kinetic operations. Criteria for case selection included availability of credible public evidence, clear attribution, and variation in context (state actors, target types). We focus on four representative cases spanning 2007–2026: (a) Operation Absolute Resolve in Venezuela, (b) Operation Orchard in Syria, (c) Targeting malware in the Donbas, and (d) the Viasat satellite attack. Each offers insight into cyber–kinetic integration with differing outcomes. For each case, we apply process tracing to reconstruct the sequence:

a. Access – How did the attacker gain a foothold (e.g. malware delivery, insider system control)?

b. Exploitation – How was that foothold used (e.g. data collection, system manipulation, denials)?

c. Kinetic Linkage – How was the cyber output tied to a physical operation (e.g. targeting orders, timing coordination)?

d. Outcome – What physical effect occurred (e.g. destruction of equipment, facilitation of a strike)?

We rely on declassified reports, cybersecurity firms, reputable media investigations, and doctrinal statements for evidence. Process tracing is ideal here: it forces us to assess both the technical chain of events and the decision-making that linked them . This process tracing is based on open-source material only, and the resulting reconstructions are therefore constrained by incomplete disclosure, uneven source quality, and the difficulty of independently verifying covert operational details. At the end we compare cases across variables (attribution certainty,

scale of effect, etc.) to draw broader conclusions. In the comparative table, evidence strength is coded as stronger where multiple independent sources converge on attribution, mechanism, and operational timing, and as moderate where one or more of those elements remain contested, indirect, or inferential.

5. Case Studies

5.1 Multi-Domain Sabotage in Operation Absolute Resolve – Venezuela (2026).

On January 3, 2026, United States military forces executed Operation Absolute Resolve, a rapid, multi-domain precision raid in Caracas that resulted in the apprehension of Venezuelan President Nicolás Maduro (Royal United Services Institute, 2026 This operation may be viewed as a contemporary and potentially important example of a Cyber-Enabled Kinetic Operation (CEKO), suggesting how offensive cyber capabilities can be combined with space effects, electronic warfare, and physical strikes to disrupt an adversary's command structure (Manohar Parrikar Institute for Defence Studies and Analyses, 2026). Rather than relying strictly on conventional kinetic devastation, the operation utilized a "layered effects" strategy directed by U.S. Cyber Command and Space Command to isolate the capital city, severing defensive communications before the physical raid package even entered Venezuelan territory (Royal United Services Institute, 2026). Process tracing highlights a tightly orchestrated cross-domain sequence:

- Access: Available accounts suggest that the digital component may have been prepared months before the physical incursion through a covert presence inside Venezuelan networks (Royal United Services Institute, 2026). U.S. cyber actors successfully mapped routines and secured persistent footholds within critical Supervisory Control and Data Acquisition (SCADA) networks—specifically targeting the Guri Dam energy distribution framework—alongside regional energy management systems and the state's smart surveillance backbone (Institute for National Security Studies, 2026).
- Exploitation: In the predawn hours of the operation, these digital vulnerabilities were actively exploited to systematically disable power grids and compromise monitoring networks (Institute for National Security Studies, 2026). Cyber-enabled access allowed U.S. forces to manipulate and observe the operational theater through Venezuela's own

security cameras, while simultaneously throwing key military hubs in Caracas into darkness and disabling localized communication linkages (Brumfield, 2026).

- Kinetic Linkage: The cyber-induced infrastructure disruption appears to have been closely synchronized with the physical deployment of Special Operations helicopters and conventional strike aircraft (Manohar Parrikar Institute for Defence Studies and Analyses, 2026). By leveraging cyber capabilities to mute defensive sensors and delay troop mobilization, planners created an unmonitored physical corridor through a formidable air defense network, enabling the ground apprehension force to breach Maduro's compound without triggering an organized military counter-response (Brumfield, 2026).
- Outcome & Operational Advantage: The core strategic objective was achieved in less than three hours, resulting in the extraction of Maduro to face federal charges in the United States (Royal United Services Institute, 2026). While early political and media narratives framed the blackout as a singular "precision cyber strike," post-operation forensic evidence revealed a more complex "cyber to blind, kinetic to break" dynamic (Brumfield, 2026). Initial digital disruptions to the grid were immediately solidified by targeted kinetic attacks—including the deployment of carbon-fiber (graphite) BLU-114/B munitions and physical raids on the Panamericana and Escuela Militar power substations—to permanently prevent the grid's recovery (Brumfield, 2026; Institute for National Security Studies, 2026). This highly integrated approach appears to have left parts of Venezuela's air defense system temporarily ineffective, or at least insufficiently responsive, during the assault (Manohar Parrikar Institute for Defence Studies and Analyses, 2026).

5.2 Radar Spoofing in Operation Orchard – Syria (2007)

On September 6, 2007, Israeli aircraft executed Operation Orchard, a kinetic airstrike that successfully destroyed a suspected clandestine nuclear reactor in the Al-Kibar region of Syria (Koch & Golling, 2016). This operation is often cited as a foundational and highly integrated example of possible CEKO, suggesting that offensive cyber capabilities can function as a force multiplier when planned and executed in tandem with conventional forces (Long, 2017). Rather than jamming the radars traditionally—which would immediately alert the adversary that an attack was underway—cyber-enabled vectors were leveraged to manipulate

the air defense data stream directly (Koch & Golling, 2016). Process tracing suggests a closely synchronized cross-domain sequence:

- Access: Available analyses suggest that attackers gained an initial foothold in the Syrian air defense network (Koch & Golling, 2016). Highly credible security analyses indicate this occurred via tailored airborne data injection or through pre-compromised supply chain vulnerabilities embedded within the commercial off-the-shelf (COTS) chips of the radar hardware components (Koch & Golling, 2016; Long, 2017).
- Exploitation: Rather than completely disabling or shutting the network down—which would trigger automated failure alerts—the cyber-electronic attack subtly manipulated the data packets processed by the radar stations (Koch & Golling, 2016). The system fed the military operators a false, completely normal data stream, displaying a peaceful, empty sky on their monitors while Israeli fighter jets breached Syrian airspace undetected (Koch & Golling, 2016).
- Kinetic Linkage: This advanced cyber-deception was precisely synchronized with the real-time flight paths and operational timeline of the approaching strike package (Long, 2017). The cyber effect opened a temporary physical corridor through the network, allowing traditional kinetic assets (F-15I and F-16I aircraft) to penetrate the airspace and drop conventional munitions directly on the tactical physical target without being noticed (Koch & Golling, 2016).
- Outcome & Operational Advantage: The physical objective was entirely destroyed, and the entire strike package returned safely to base without Syria firing a single surface-to-air missile (Koch & Golling, 2016). If this cyber-spoofing component functioned as reported, it likely reduced the need to contest heavily defended airspace and may have lowered the risk of mission failure, aircraft losses, and wider escalation (Long, 2017).

5.3 Targeting Ukrainian Artillery – Donbas (2014–2016)

In late 2014, amid the war in Donbas, Russian military intelligence (GRU) reportedly utilized a trojanized Android application to conduct tactical reconnaissance against Ukrainian artillery assets (CrowdStrike, 2017). A legitimate mobile application designed by a Ukrainian officer to reduce processing times for Soviet-era D-30 towed howitzers was injected with an "X-Agent" malware implant linked to the threat actor group Fancy Bear (CrowdStrike, 2017). While this case has frequently been cited as a foundational real-world example of a cyber-

enabled kinetic operation, its empirical validity remains highly contested, offering an instructive lesson in the methodological difficulties of cross-domain combat verification (Voice of America, 2017). Process tracing outlines the alleged operational sequence alongside its subsequent evidentiary disputes:

- Access: The adversary covertly distributed the malicious Android Package (APK) on Ukrainian military forums between late 2014 and 2016 (CrowdStrike, 2017). Artillery personnel downloading the calculation application unknowingly granted the implant deep system privileges.
- Exploitation: Once installed, the X-Agent variant was technically capable of exfiltrating communications, contacts, device metadata, and gross geographical location data from the infected mobile devices back to hostile command-and-control servers (CrowdStrike, 2017).
- Kinetic Linkage: In theory, this locational data was designed to act as a target beacon, allowing Russian front-line forces to coordinate real-time missile and counter-battery artillery strikes against exposed Ukrainian firing positions (CrowdStrike, 2017). Early analytical models posited that this digital espionage directly shortened the adversary's find-to-engage loop on the battlefield.
- Outcome & Operational Advantage: The operational outcome of this intersection remains deeply disputed. In its initial December 2016 brief, CrowdStrike asserted that the malware directly contributed to the catastrophic destruction of over 80% of Ukraine's D-30 howitzer fleet (Voice of America, 2017). However, in March 2017, the firm heavily revised and walked back its core conclusions following formal pushback (Voice of America, 2017). The Ukrainian Ministry of Defense flatly rejected the assertions, stating that actual combat artillery losses were multiple times smaller and entirely unrelated to mobile device compromise (The Peninsula Qatar, 2017). Furthermore, the International Institute for Strategic Studies (IISS) disavowed the misinterpretation of its data, forcing CrowdStrike to formally excise language claiming that the malware contributed to high battlefield asset losses (Voice of America, 2017). Consequently, rather than serving as a confirmed textbook CEKO, the Donbas artillery case functions as a vital theoretical blueprint of potential cross-domain linkage whose real-world lethality lacks verified confirmation.

5.4 Satellite Communications Disruption – Ukraine (2022)

On February 24, 2022, precisely coinciding with the launch of the Russian military's full-scale ground invasion of Ukraine, state-sponsored cyber actors executed a highly disruptive attack against Viasat's KA-SAT satellite broadband network infrastructure (European Union, 2022). This operation may be viewed as a particularly well-documented example of a Cyber-Enabled Kinetic Operation (CEKO), intentionally designed to degrade and paralyze Ukrainian tactical military communications mere minutes before the initial conventional assault commenced (European Union, 2022). By aggressively targeting a commercial satellite communication framework that actively underpinned the state's territorial air defenses and troop command networks, the cyber mission worked explicitly to prepare the physical battlefield for the incoming multi-domain offensive (European Union, 2022). Process tracing reveals a precisely timed cross-domain sequence:

- Access: In the weeks preceding the kinetic incursion, the threat actors mapped out the target's network topology to exploit vulnerabilities within the ground segment of the communication architecture (Viasat, 2022). Hostile entities successfully penetrated the satellite network infrastructure through a management center installation, securing the initial administrative footholds required to push commands to connected remote units (Guerrero-Saade, 2022).
- Exploitation: Once inside the terminal management systems, the attackers deployed a novel, highly destructive MIPS architecture wiper malware sample known as "AcidRain" (Guerrero-Saade, 2022). Rather than conducting passive espionage, the attackers remotely detonated this malicious firmware on user modems, systematically wiping the terminal flash memory and leaving thousands of satellite terminals permanently inoperable and unresponsive (Guerrero-Saade, 2022).
- Kinetic Linkage: This massive digital disruption was carefully synchronized with the exact opening hours of the multi-front conventional invasion (European Union, 2022). The widespread wiping of the ground terminals was executed to directly impair and blackout Ukrainian command-and-control (C2) coordination chains right as physical tanks crossed borders and conventional artillery barrages were initiated (European Union, 2022; Guerrero-Saade, 2022).

- Outcome & Operational Advantage: The immediate impact of the digital strike likely yielded a broad, asymmetric kinetic advantage for the invading forces during the critical early hours of the war (European Union, 2022). The instantaneous loss of secure connectivity appeared to have severely compromised real-time military communication channels, blinding local air defense monitoring cells and heavily delaying front-line troop coordination efforts (European Union, 2022). Formal public attribution for this destructive cross-domain operation is highly certain, following a coordinated international declaration by Western allied governments explicitly identifying the Russian state as the responsible belligerent (European Union, 2022).

6. Comparative Analysis

Tabel 1: A Comparative Analysis of CEKO

Case / Year	Evidence Strength	Attribution	Cyber Role	Kinetic Outcome
Operation Absolute Resolve – Venezuela (2026)	Strong(converging open-source analyses and official commentary)	United States (U.S. Cyber Command / Space Command)	Persistent SCADA network exploitation (Guri Dam), smart surveillance manipulation, and real-time C2 isolation	Air defenses significantly degraded; power substations permanently disabled via BLU-114/B graphite munitions; extraction of Maduro
Operation Orchard– Syria (2007)	Moderate to Strong(Declassified intelligence / forensic technical data)	Israel (Unacknowledged)	Active radar data stream manipulation and data packet spoofing	Air defense tracking arrays blinded; clandestine nuclear facility completely destroyed via tactical airstrike
Donbas – Ukraine (2014–16)	Moderate(Cyber forensics / data heavily contested	Russia (APT28 / GRU)	Tactical reconnaissance/ espionage via malicious Android implants	Geolocation exposure of Ukrainian D-30 artillery units to counter-battery rocket/missile fire

Case / Year	Evidence Strength	Attribution	Cyber Role	Kinetic Outcome
	by UKR MoD)			
Viasat – Ukraine (2022)	Strong(Coordinated international allied public attribution)	Russia (GRU / FSB)	Immediate Denial of Service via "AcidRain" wiper deployment on civilian/military modems	Severe disruption to tactical military command-and-control communications during the initial hours of physical invasion

Source: Created by Author

This table highlights how CEKO cases vary across the operational spectrum. Operation Absolute Resolve and Operation Orchard appear to offer relatively strong evidence of cyber–kinetic integration, although parts of the causal chain remain inferential and should be treated with caution. The Ukrainian artillery case remains analytically instructive, but both attribution and the scale of any kinetic effect are contested, even though unclassified public sources stop short of naming specific destroyed hardware units.

Several patterns emerge from this comparative dataset::

- Access Complexity: The cases examined here suggest that CEKO often require extensive pre-planning and advanced cyber exploitation methods, such as deep SCADA network mapping, customized mobile application implants, or satellite network infrastructure breaches. These interventions were not spur-of-the-moment hacks; rather, they required sustained, covert technical campaigns orchestrated by sophisticated state-backed actors.
- Integration: In Operation Absolute Resolve, Operation Orchard, and the Viasat disruption, cyber operations and kinetic maneuvers were tightly integrated under a centralized joint command structure. The Donbas artillery case demonstrates partial cross-domain integration, linking independent cyber intelligence units directly with active front-line military artillery teams.
- Outcomes: In the cases assessed here, stronger CEKO claims are associated with measurable physical effects—such as hard equipment destruction or total

communication failure—that directly corresponds to the targeted cyber action. In weaker instances, cyber attacks merely set generalized background conditions, such as isolating non-military networks, without delivering a definitive or synchronized kinetic follow-through

Ultimately, these empirical findings validate the foundational Rid-Libicki perspective that cyber power's primary utility on the modern battlefield is preparatory and environmental rather than independently decisive. However, by isolating CEKO as a discrete sub-category, the cases suggest that when offensive cyber capabilities are closely integrated within a multi-domain kill chain, they may contribute materially to high-impact physical outcomes alongside conventional force.

7. Conceptual Insights and Recommendations

7.1 Theoretical Implications.

Our analysis suggests that CEKO are neither inevitable nor easily achieved. They require both sophisticated capability and a political-military willingness to closely integrate cyber with firepower. Conceptually, CEKO can be seen as an extension of network-centric warfare and cognitive warfare theories. Like electronic warfare in WWII or air interdiction in Korea, they aim to degrade enemy decision cycles. They rely on situational awareness advantages and precise timing. Ole Wæver’s securitization theory reminds us that declaring cyberspace a domain (as NATO did) is a political act; recognizing CEKO as a distinct category may likewise require doctrinal securitization.

We propose refined set of working criteria for CEKO: a state must (a) target a system that is instrumental to an enemy military function, (b) have reliable, persistent access to that system, (c) integrate cyber planning with the physical attack timeline, and (d) achieve a measurable physical effect. If any condition fails, the operation falls outside our CEKO definition. For example, broad ransomware in wartime economy does not count; disabling a radar in flight path planning does. These boundaries help operationalize CEKO for policymakers and legal scholars: only operations meeting these criteria should be analyzed as cross-domain warfare, with attendant escalation and legal considerations.

7.2 Policy and Doctrinal Recommendations. Based on the cases above, we recommend:

- Clarify CEKO in Doctrine: Official doctrines (e.g. updated JP 3-0, NATO concepts) should explicitly define cyber-enabled vs. independent operations, drawing where useful on the working criteria proposed here. This will help commanders recognize opportunities and limits.
- Invest in Resilience: Because CEKO can yield significant advantage, defenders must harden critical systems. For example, isolating military C2 networks (as Ukraine did for key data centers) and requiring physical security for vital cyber nodes.
- Improve Joint Planning: Training and wargames should routinely include cyber-kinetic scenarios. As Borghard et al. argue, all warfighters need familiarity with cyber's battlefield role. Exercises can test process-tracing conditions (access, exploitation, linkage) to ensure integration.
- Develop Targeting Guidance: Legal frameworks (like the Tallinn Manual on armed conflict) should consider CEKO specifics, e.g. when a cyber-facilitated strike is a single blended attack requiring proportional response.
- Strategic Deception and Endurance: Since defenses are improving, attackers and defenders will engage in cyber "lapsus" akin to electronic warfare. Emphasis should shift to redundancy and deception – for instance, feeding false data (Operation Orchard style) can be potent.

8. Conclusion

In sum, Cyber-Enabled Kinetic Operations can be treated as a distinct analytical phenomenon, but they are neither pervasive nor straightforward. High-profile examples show they can achieve significant surprise effects, but they require exceptional effort and often remain secret. The broader empirical record – from Syria to Ukraine – indicates that most cyberattacks in wartime serve supporting roles (espionage, disruption, information) rather than directly pulling the trigger on bombs or missiles. By clearly defining CEKO and analyzing key cases, this paper lays groundwork for further research and better doctrine. The primary contribution is therefore conceptual, while the four cases function as illustrative applications of the framework rather than as a comprehensive empirical base for universal claims. Future conflicts may see more CEKO as technology advances (e.g. 5G, AI) and doctrines mature, but for now the threshold between cyber and kinetic warfare remains high. Recognizing that boundary, as we have endeavoured to do, is essential for informed strategy and policy.

References

Bonner, T. (2014). Cyber power integration in joint operations (Monograph). U.S. Army Command and General Staff College.

Borghard, E. D., & Lonergan, S. W. (2021). Cyber operations as instruments of statecraft: Evidence from the United States and Russia. Strategic Studies Quarterly, 15(1), 101–124.

Brumfield, C. (2026, February 19). The Caracas operation suggests cyber was part of the plan – just not the whole operation. CyberScoop. https://cyberscoop.com/venezuela-blackout-cyberattack-vs-kinetic-damage-operation-absolute-resolve/

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

CrowdStrike. (2017, March 23). Use of Fancy Bear Android malware in tracking of Ukrainian field artillery units (White Paper). CrowdStrike. https://www.crowdstrike.com/wp-content/brochures/fancy-bear/FancyBearTracksUkrainianArtillery.pdf

European Union. (2022, May 10). Russian cyberoperations against Ukraine: Declaration by the High Representative on behalf of the European Union [Press release]. Council of the European Union. https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyberoperations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

George, A. L., & Bennett, A. (2005). Case studies and theory development in the social sciences. MIT Press.

Guerrero-Saade, J. A. (2022, March 31). AcidRain: A modem wiper rains down on Europe. SentinelLabs. https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

Institute for National Security Studies. (2026, January 12). Did the United States Strike the Power Grid During the Operation in Venezuela? INSS Insight. https://www.inss.org.il/social_media/did-the-united-states-strike-the-power-grid-during-the-operation-in-venezuela/

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. International Security, 38(2), 7–40. https://doi.org/10.1162/ISEC_a_00138

Koch, R., & Golling, M. (2016). Weapons systems and cyber security - a challenging union. 2016 8th International Conference on Cyber Conflict (CyCon), 191–203. https://doi.org/10.1109/cycon.2016.7529435

Libicki, M. C. (2020). Cyberspace in peace and war (2nd ed.). Naval Institute Press.

Lindsay, J. R. (2015). Tipping the scales: The strategic asymmetry of business and military cyber espionage. Intelligence and National Security, 30(2-3), 254–287. https://doi.org/10.1080/02684527.2014.985323

Long, A. (2017). A cyber SIOP? Operational considerations for strategic offensive cyber planning. Journal of Cybersecurity, 3(1), 17–28. https://doi.org/10.1093/cybsec/tyw016

Manohar Parrikar Institute for Defence Studies and Analyses. (2026, January 13). Operation Absolute Resolve and the Future of Warfare: Military Lessons for India. MP-IDSA Issue Brief. https://idsa.in/publisher/issuebrief/operation-absolute-resolve-and-the-future-of-warfare-military-lessons-for-india

The Peninsula Qatar. (2017, January 6). Ukraine military denies Russian hack attack. https://thepeninsulaqatar.com/article/06/01/2017/Ukraine-military-denies-Russian-hack-attack

Rid, T. (2012). Cyber war will not take place. Journal of Strategic Studies, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Royal United Services Institute. (2026, January 14). Layered Ambiguity: US Cyber Capabilities in the Raid to Extract Maduro from Venezuela. RUSI Commentary. https://my.rusi.org/resource/layered-ambiguity-us-cyber-capabilities-in-the-raid-to-extract-maduro-from-venezuela.html

Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber coercion: The threat of cyber conflict. Oxford University Press.

Viasat. (2022, March 30). KA-SAT network cyber event update. Viasat Corporate Blog. https://www.viasat.com/space-innovation/cyber-security/ka-sat-network-cyber-event-update/

Voice of America. (2017, March 23). Cyber firm rewrites part of disputed Russian hacking report. VOA News. https://www.voanews.com/a/cyber-firm-rewrites-part-disputed-russian-hacking-report/3781411.html