Cross-domain concerns

Defeating a hybrid state's grand strategy

By Victor Morris

This article analyzes joint and multinational wargames designed to understand, mitigate and overcome dilemmas preventing long-term mission success. These dilemmas are at both the operational and strategic levels and are associated with the contemporary operational environment, multinational alliances and hybrid threat actors. The analysis also identified implications for NATO crisis response planning associated with a hybrid state's strategy.

State and non-state competitors develop strategies across competition continuum relative to rival advantages. The competition continuum consists of cooperation, competition below armed conflict, and armed conflict.[1] The resulting strategies emphasizes both direct and indirect approaches across all domains to reach strategic ends. A domain is defined as a critical macro maneuver space whose access or control is vital to the freedom of action and superiority required by the mission."[2] The domains included in this assessment are human, land, air, sea, space and cyber. Dense urban, information and electromagnetic environments are also overlapping spaces for military and non-military effects.

Cross-domain effects are accelerated by hybrid states and non-state actors. Hybrid states are described as states with a mix of autocratic and democratic features. This assessment uses the term "hybrid state" to describe a state blurring boundaries between organizations and institutions[3] enabling an unbounded grand strategy. This type of state also has low competition in elections and low constraints on governmental power. These characteristics facilitate statecraft and unbounded policy to offset perceived disadvantages, deliver key narratives and shape international norms.

Target states must understand the operational environment, cross-domain effects and evolving character of war to develop resilience to both direct and indirect approaches of the strategy. It is imperative this comprehensive understanding of the operational environment encompasses planning considerations including geopolitical rival or competitor's critical factors enabling strategic purposes and shifts to parity. Critical factors are the critical capabilities, requirements and vulnerabilities associated with interrelated centers of gravity (COGs).[4] COGs are the "doer"[5] or physical agents possessing the ability to achieve objectives.

The following lessons outline how a hybrid state builds its grand strategy and what critical factors it considers offsetting disadvantages. The lessons also elucidate countermeasures targeting vulnerabilities and enabling resilience to multi-domain drivers of conflict. The goal of the below assessment is identifying friendly and adversary critical vulnerabilities for engagement and conditions change.

Wargame lessons learned prioritize a geopolitical rival's indirect approach using enhanced proxy forces as a significant advantage and long-term dilemma for NATO and key partner nations. Waging so-called "Hybrid Warfare" within a grand strategy requires conducting political, conventional, unconventional, asymmetric, proxy and cyber warfare to both directly and indirectly influence objectives across all domains and instruments of national power.

1. A hybrid state develops an unbounded grand strategy across the competition continuum relative to perceived rival advantages.

Fundamentally, the western multi-domain operations concept acknowledges the competition continuum and involves achieving positions of relative advantage through joint reconnaissance, offensive and defensive operations. Limited stability operations and a whole of government approach are designed to consolidate gains and enable operational and strategic ends. Precision air, ground and naval fires, coupled with effective means of intelligence collection are advantages enabling effective large scale combat operations. The rival's grand strategy accounts for these advantages preventing their strategic ends. Every strategy has ends, ways and means interrelated with critical factors. Because ends, ways and means have limitations, indirect approaches reduce disadvantages and allow innovative alternatives oriented towards opponent COGs. A peer or near peer competitor operationalizes a hybrid approach through mixed threat actors operating across all domains.

Therefore, shaping campaigns with subversive actors prior to, or in concert with conventional force are critical strengths for the adversary. This refers to limited or major joint operations employing multiple forms of warfare across all domains to enable decisive conditions and affect. Manipulating national and international policy using fluctuating diplomatic, informational and economic elements of national power supported by overt, covert and/or un-attributable offensive options are also critical factors for deep operations.

Next, offensive options involve combined arms direct and indirect fires and electronic warfare capabilities. Cyber, electromagnetic and information environmental effects are technologically accelerated in this type of strategy and prioritized to affect the depth of the adversary's operational environment. The threat of nuclear weapons employment and large-scale military force capabilities reinforce deterrence and influence the near-abroad, and international community.

Furthermore, proxy organizations present significant dilemmas for joint and multinational alliances when used as a key component of an unbounded grand strategy. Proxy organizations, however, are not limited to non-state paramilitary or insurgent networks. These un-attributable groups also include convergent terrorist,

1 *McCoy, Kelly (2018, April). In the Beginning, There Was Competition: The Old Idea Behind the New American Way of War. Article retrieved from https://mwi.usma.edu/beginning-competition-old-idea-behind-new-american-way-war/*

2 *Donnelley, Jared and Farley, Jon (2018, September). Defining the "Domain" in Multi Domain. Article retrieved from https://othjournal.com/2018/09/17/defining-the-domain-in-multi-domain/*

3 *Galeotti, Mark (2016, December). Russia's Hybrid War as a Byproduct of a Hybrid State. Article retrieved from https://warontherocks.com/2016/12/russias-hybrid-war-as-a-byproduct-of-a-hybrid-state/*

4 *Strange, Joe (1996). Center of Gravity and Critical Vulnerabilities. Article retrieved from http://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/3B_COG_and_Critical_Vulnerabilities.pdf*

5 *Eikmeier, Dale (2016, October). Let's Fix or Kill the Center of Gravity Concept. Article retrieved from http://ndupress.ndu.edu/Media/News/Article/969689/lets-fix-or-kill-the-center-of-gravity-concept/*

Soldiers assigned to Company A, 1st Battalion, 155th Infantry Regiment, 155th Armored Brigade Combat Team, Task Force Spartan, bound toward an objective during a rehearsal for a combined live-fire exercise near Alexandria, Egypt, Sept. 10, 2018. The 155th ABCT took part in exercise Bright Star 18, a multilateral U.S. Central Command training exercise. (Sgt. James Lefty Larimer/U.S. Army)

transnational organized crime and international hacker organizations. Multinational companies, political parties and civic groups also act as proxy organizations with access to high-end technologies and capabilities. These organizations cooperate or compete with other proxy actors based on various motivations. All or some of these groups may be enabled or incentivized by the hybrid state or local population providing sanctuary for them. Regardless, the need to deliberately expand sanctuaries over time is a critical requirement and potential critical vulnerability.

Potential dilemmas for NATO military operations involve irregular and asymmetric warfare activities in member states against borderless proxy actors, during or after an Article V response and territorial restoration campaign. As mentioned earlier, both asymmetric and conventional operations occurring linearly or non-linearly across all domains and are included in the hybrid state's grand strategy as critical strengths. The battlespace may also vary between contiguous and non-contiguous physical terrain. Un-attributable proxy forces with access to emerging and disruptive technologies support the hybrid state's critical capability to accelerate both indirect and asymmetric campaigns, whilst assessing the effects of long-term lawfare and political warfare activities. Conventional limited military campaigns are also accelerated under unbounded policy to leverage vulnerabilities and manipulate non-military settlements.

Critical factors not translating across all institutions and levels of policy are mitigated by several combinations. For instance, supra-national, supra-domain, supra-tier and supra-means combinations[6] as well as non-linear systems behavior ensure effects escalation and third order effects. For example, supra-national combinations are a synthesis of national, international and non-state organizations.

To summarize, a hybrid state's critical factors are contained in complex systems capable of delivering effects across the competition continuum. The systems 1) conventional joint and irregular proxy forces with integrated air, ground and sea defense

6 *Liang, Qiao and Xiangsui Wang (1999, February). Unrestricted Warfare. Art Publishing House.*

capabilities, 2) emerging and disruptive technologies and 3) super-empowered individuals conducting subversive activities. Subversive organizations cooperate and compete in all domains to exploit vulnerabilities of targeted states.

Based on the above analysis, critical vulnerabilities are identified. Some adversary critical vulnerabilities are subversive state or non-state actors, combined arms tactical groups, proxy sanctuary and malicious information campaigns. From a NATO perspective, counter-irregular or hybrid warfare dilemmas include a variety of factors during states of exception, emergency and war.

The remaining two sections outline direct and indirect targeting of rival critical vulnerabilities to develop resilience to drivers of hybrid conflict. Identifying and transforming friendly critical vulnerabilities through self-assessment are also included to counter a hybrid state's grand strategy.

2. Conduct joint, bilateral and multinational collaborative planning early and often.

Understanding multinational systems is a key aspect of friendly or blue force critical factors analysis. Early and recurring collaborative planning is crucial to joint operations and assessment processes that fuel multi-level shaping and crisis response activities. Equally important for political level contingency planning is understanding an adversary's strategy employing indirect approaches and use of asymmetric proxies to reach objectives.[7] These objectives extend beyond the joint operation plan and hinge on limited military activities and frozen conflicts as desired end states. Reaching these objectives within a NATO member state or region presents even more complex dilemmas and lasting effects for the international community and alliance cohesion. An indirect or "Gray Zone" approach is more immune to NATO collective defense and strategic deterrence planning. The Gray Zone is "the hostile or adversarial interactions among competing actors below the threshold of conventional war and above the threshold of peaceful competition."[8] This approach also exploits seams in the competition continuum involving dual cooperation and competition in geo-politics and economic systems. The hybrid state's ultimate objectives are to discredit and degrade the target's governance and societal cohesion. These objectives are met through sustained lawfare and irregular warfare activities and operations. Lawfare misuses or manipulates the law for political or military objectives, effectively using the legal system against an adversary to delegitimize them.

Additionally, every citizen needs to be educated and prepared for resistance and role in hybrid defense[9] which includes deliberate planning and cumulative innovation. Populations must enable interorganizational resilience across the continuum of government and competition spectrums. NATO, European Union and United Nations partnerships are critical requirements for collective defense and deterrence. During states of exception, emergency or war it is imperative to synchronize unified action partners. These include law enforcement, special operations, volunteer defense and home guard forces in key support, close and deep areas.

Next, collective defense treaties and joint security cooperation consists of both foreign internal defense and security force assistance to shape and prevent conflict. Foreign internal defense when approved involves combat operations during a state of war, where offensive, counteroffensive or counterattacks enable forces to regain the initiative. Thus, defensive tasks are a counter to the enemy offense, while protection determines which potential threats disrupt operations and then counters or mitigates those threats. Examples of specific threats include explosive hazards, improvised weapons, unmanned aerial and ground systems, and weapons of mass destruction.

Defeating the enemy and consolidating gains inherently involves more forces and is an operational headquarters planning requirement. Specific requirements include joint force assignment, apportionment, contingency and execution sourcing. Additionally, adversary related Anti-access Area Denial (A2/AD) capabilities consisting of integrated multi-domain defense systems are a joint problem. They require joint capabilities to exploit windows of superiority, freedom of action and gains consolidation to revise, maintain or cancel the plan.

3. Get closer to the ground truth in the human domain and prepare for human-machine teaming.

World-class intelligence, surveillance, target acquisition and reconnaissance capabilities should not overshadow critical capabilities and requirements for security services, law enforcement and indigenous population intelligence development. Sharing intelligence is equally as important and inevitably involves interoperable intelligence functional services and shared databases. Multinational counterintelligence, human intelligence and identity intelligence sharing agreements must be refined and validated down to the tactical level adequately ensuring all that relevant intelligence disciplines are processed and disseminated in a timely manner.

Furthermore, mission command through human-machine teaming is inevitable and will undoubtedly leverage human adaptability, automated speed and precision as future critical factors. The global competition for machine intelligence dominance will also become a key element of both the changing character of war and technical threat to strategic stability.

Scenarios and wargames designed to force multi-national COG and critical factors analysis, decision making and assessments are critical to understanding 21st century conflict. The joint operational area must be assessed as one interconnected domain and put in the correct context to assess the level of military effort and where required service targets in domains that enable the land component to reach strategic objectives. The interconnected domain is where conventional, asymmetric, criminal and cyber activities occur at the same time in the same spaces with predictable and unpredictable effects. A long-term indirect and proxy-led approach within the hybrid state's grand strategy offers innovative, inexpensive and unbounded opportunities to reach geopolitical objectives below the threshold of armed conflict.

Victor Morris is a former military officer, irregular warfare and counter-improvised explosive device instructor at the Joint Multinational Readiness Center in Germany. He has conducted partnered training in 17 European nations, with four NATO centers of excellence, and at the NATO Joint Warfare Center. The views expressed in this article are based on the author's observations alone and do not reflect the official policies of any mentioned organizations.

7 *Mumford, Andrew (2017, November). The New Era of the Proliferated Proxy War. Article retrieved from https://thestrategybridge.org/the-bridge/2017/11/16/the-new-era-of-the-proliferated-proxy-war*

8 *Morris, Victor R. (2018, May). Quanta of Competition: Quantum Mechanics, Multi-Domain Battle, and the Gray Zone (Part I). Article retrieved from https://othjournal.com/2018/05/14/quanta-of-competition-quantum-mechanics-multi-domain-battle-and-the-gray-zone-part-i/*

9 *Galeotti, Mark (2015, July). Time to Think About "Hybrid Defense". Article retrieved from https://warontherocks.com/2015/07/time-to-think-about-hybrid-defense/*