Intelligence Policy Considerations in Large-Scale Combat Operations

by Mr. Gregory Hatter, Mr. Scott Schultz,
Mr. Craig Bell, Colonel Lisa Walker,
and Colonel Bill Mangan

Introduction

The purpose of policy is to direct and assign tasks, prescribe desired capabilities, and provide guidance for ensuring the armed forces are prepared to execute operations. The *Merriam-Webster Dictionary* defines policy as "prudence of wisdom in the management of affairs."[1]

We often hear, "We need to change our policy," but is this always a valid statement? Probably not, particularly if one considers the times we use it interchangeably with rules of engagement, authorities, roles and functions, or even doctrine. However, when considering multi-domain operations and large-scale combat operations, this statement is invaluable. It should trigger the critical thought necessary to apply "prudence of wisdom" to our intelligence policies now, so that we will be able to fight and win in the future and not be frustrated with "policies" that are not fit for purpose and are late to need.
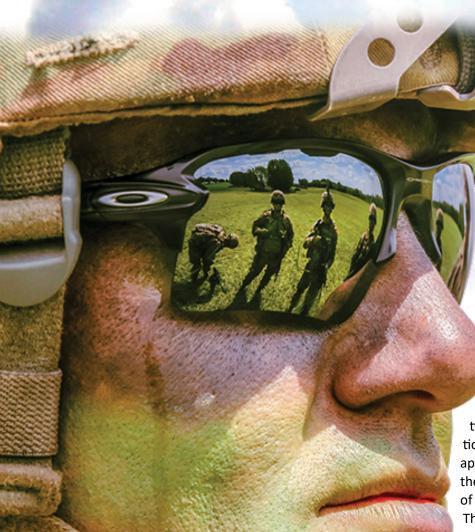
Intelligence Policies

The problem with intelligence policy in support of multi-domain operations and large-scale combat operations should not start with a wholesale review of those "on-the-shelf" policies or the binary question of "do we have one or not?" It is more appropriate to consider the problem operationally. As an intelligence formation, we should think about our policies in terms of time, space, unity of purpose, and threat focus.

Our pacing threats operate relentlessly across a broad geographic area and in multiple domains. The Russian center of gravity in our "competition" phase is the integration of information warfare, the integration of unconventional warfare, and the application of conventional forces. During the "conflict" phase, the Russians' center of gravity is their long- and mid-range fires. Thinking through the defeat of the Russian center of gravity by phase should trigger immediate thoughts as to policy adequacy for intelligence practioners.

Army SGT Samuel Benton observes and mentors soldiers during the Bull Run V training exercise with Battle Group Poland in Olecko, Poland, May 22, 2018. Battle Group Poland includes United States, United Kingdom, Croatian, and Romanian soldiers who support NATO's enhanced forward presence.

The layered standoff problems of multi-domain operations center on the joint force's ability to compete so as to defeat an adversary's operations to destabilize; deter the escalation of violence; and if there is an escalation, enable a rapid transition to armed conflict. During this rapid transition, the joint force must be able to—

✦ penetrate antiaccess and area denial technology,

✦ dis-integrate antiaccess and area denial to enable friendly maneuver,

✦ exploit the resulting freedom of maneuver, and

✦ recompete to consolidate gains.

This problem set has a host of specified and implied intelligence tasks—notably, the task to ensure our intelligence policies enable our units to compete and then transition rapidly to conflict. Failure to have adequate policies in place increases the risk of being late to need. Undoubtedly, some may say, "If the fighting starts, we will be able to make the changes necessary." This is clearly an assumption, but is this assumption valid? Given that our pacing threats are operating on interior lines, it is challenging for us to maintain the initiative on decision making when initiating conflict; to determine an acceptable end state or frozen conflict; and to enable commanders to make decisions using ambiguous rather than unambiguous warning information. Therefore, this assumption may not be valid at all.

As a formation, we should ask ourselves, what intelligence policies should we keep, get rid of, or modify? This question requires closer examination. Do these policies enable U.S. forces to keep pace in the transition between competition and conflict? Are they adequate at echelon? For those at home station and training or in exercises, rather than geographically engaged in the competition phase, are the policies adequate to allow their rapid transition into conflict?

These questions apply at echelon and across all intelligence disciplines. When asked, some common areas immediately come to mind regardless of the audience. A quick discussion of each helps to energize the thought process. These areas are—

✦ foreign disclosure,

✦ counterintelligence (CI) and human intelligence (HUMINT) operations, and

✦ signals intelligence (SIGINT) Soldiers and contract linguists operating in SIGINT facilities.

Foreign Disclosure

A recurring thread in our national strategy documents is the recognition that competition with near-peer threats will require us to work more closely with our allies and partners. We need to be able to share intelligence and operational information with a wide array of countries—a challenge many units already face today in myriad worldwide operations, engagements, and exercises. Foreign disclosure refers to what information a partner nation or international organization can know, in accordance with the National Disclosure Policy (NDP-1). NDP-1 establishes disclosure authorities by country, classification level, and category or type of information. Instances will always exist in which not all the same information may be disclosed to all partner nations; "writing for release" becomes paramount and must be considered as a primary planning requirement. Foreign disclosure

officers are responsible for advising units on the implementation of NDP-1 and must be involved early in the planning stage.

Several units have already included foreign disclosure guidelines in orders. The next update to FM 6-0, *Commander and Staff Organization and Operations*, should formalize this process, with an appendix dedicated to foreign disclosure and a template for a foreign disclosure annex to plans and orders. The intent of the disclosure annex is to change our mind-set and incorporate foreign disclosure throughout the planning process instead of after the fact. Many of us have experience with operation orders written at the level of Not Releasable to Foreign Nationals (NOFORN), limiting our ability to share key operational information with allies. We need to work with personnel across the staff to ensure foreign disclosure does not have the appearance of being "just" an intelligence or security function, but rather a combat multiplier.

> **" '**Writing for release' becomes paramount and must be considered as a primary planning requirement.**"**

Outside the rule set of NDP-1, an additional challenge we often face in multinational operations is the need to share national intelligence information. This often requires detailed and sometimes lengthy coordination with the national agencies who own the information. To this end, we have proposed additional verbiage for the Director of National Intelligence's *Consolidated Intelligence Guidance* to help emphasize the need and ways to share with our multinational partners.

NDP-1 is rules-based but includes the ability to request exceptions. The proper application of the provisions of NDP-1 facilitates the timely disclosure of classified military information to allied and partner nations. The question to consider is whether foreign disclosure policies are in place, understood, and trained at all echelons to keep pace in the transition between competition and conflict. On the surface, NDP-1 is enabling and has driven change to doctrine as well as inputs to the latest version of the *Consolidated Intelligence Guidance*, but is this enough?

> **"** Are we being rigorous enough to ensure our CI and HUMINT policies are adequate to achieve the end state we desire?**"**

Counterintelligence and Human Intelligence Operations

The challenges of working in a partnered environment carry over to discussions of CI and HUMINT in future large-scale combat operations against a near-peer threat. While the mantra of "write to release" needs to continue to be part of our training for collectors, we also need to review the policies driving the classification of our tradecraft to better facilitate partnering during the collection process, whether in CI or HUMINT operations, including intelligence interrogations.

Perhaps the biggest constraint we need to relook for CI and HUMINT are the authorities that allow units and personnel to conduct CI or HUMINT operations. Some CI and HUMINT forces require the authority to conduct operations outside a theater of conflict. Successful source development requires identifying potential sources in advance of need and may involve operations in an area that has not yet transitioned into conflict. Army G-2 is looking at ways to expand CI and HUMINT collection authorities. It is encouraging increased coordination between U.S. Army Forces Command, Army Reserve, and Army National Guard Forces with organizations possessing operational authorities, such as Army Service component commands and U.S. Army Intelligence and Security Command, to maximize the use of our limited forces. This proposed increase in utilization, combined with a more sophisticated adversary, also highlights the need for more forces to receive intermediate and advanced training and certification, to include operating in the cyberspace environment. This also requires better training of our leaders so that they understand the processes and discipline-specific authorities associated with expanded use of our CI and HUMINT personnel. While this process will take an initial investment of time and resources, it will allow us to better posture our forces to collect intelligence effectively and to protect our formations throughout the competition and conflict phases.

A number of questions persist and operational formations can best inform the necessary adjustment to policy. This may be about operating in the competition phase alongside multinational partners or regarding units conducting home station training rather than being geographically engaged in the competition phase. Simply put, are we being rigorous enough to ensure our CI and HUMINT policies are adequate to achieve the end state we desire?

SIGINT Soldiers and Contract Linguists Operating in SIGINT facilities

An everyday issue that confronts the SIGINT community centers on the reciprocity security screening process that causes a significant number of Soldiers and contract linguists to wait for access to the National Security Agency's (NSA) systems and facilities. Many of the Soldiers and contract linguists under security/background investigation by NSA's Military Affairs Division (MAD) are the best linguists available but are unable to support the mission until NSA completes their investigation. Most of the Soldiers will undergo their MAD assessment within a few weeks and be able to enter NSA facilities and access the NSA systems. However, Soldiers with significant foreign national affiliations receive a more extensive MAD assessment, which can take months longer to complete. Requiring Soldiers to await facility or systems access significantly degrades our ability to support the mission and/or train on the systems needed to support large-scale combat operations and multi-domain operations during the competition phase.

This policy challenge confronts us daily in the competition phase. The Office of the Chief of Military Intelligence is addressing this issue of MAD reciprocity process by changing DA PAM 611-21, *Military Occupational Classification and Structure*, to modify the qualifications to hold a SIGINT military occupational specialty. This policy change will reduce the number of Soldiers waiting long periods for access to facilities and systems and reduce the MAD backlog of Soldiers awaiting MAD assessments.

MAD processing has a more significant impact on the contract linguist population. Almost all the contract linguists have foreign national affiliation issues, and the MAD often requires them to undergo an extensive CI assessment that can take more than a year. This lengthy MAD assessment process can affect the ability to use contract linguists to support surge operations as well as the number of contract linguists available to support operations during the competition phase. This issue negates the use of contract linguists to provide a surge capability until we can either recruit or train more Soldiers to fill gaps in our formations and exac-erbates our challenge of rapidly transitioning from competition to conflict. Army G-2 is working with the MAD and the NSA CI assessment team to identify efficiencies to accelerate the MAD process for contract linguists and reduce the length of time these linguists spend awaiting a favorable MAD assessment.

In the SIGINT realm, the focus has been on adapting to the policies in place rather than changing the policies themselves. This may be adequate, but is it sufficiently adequate to keep pace in the transition between competition and conflict? It is too early to tell if the policy changes we are making will reduce the number of Soldiers and contract linguists who are awaiting facility or systems access. Even if the policy changes we are making are effective, we need to consider the impact of not using our best (military and contract) linguists to support operations during the competition and the conflict phases. This is a policy issue we need to address now in order to have sufficient linguist capacity available for training and to support critical missions during the competition phase.

Conclusion

The emerging multi-domain operational environment reflects adversaries that are expanding their efforts to reduce friendly force decision-making time, operating across domains and at echelon, and engaging geographically where our allies and partners live. The lines are becoming blurrier between "below armed conflict" and conflict. The complexity and criticality of the competition phase is arguably on par with the conflict phase. Whether one is looking for changes to authorities, rules of engagement, roles and functions, or even doctrine, policy considerations are either foundational or a critical driver. A rigorous interrogation of our current policy stance across all intelligence disciplines and the prudence of wisdom in making and applying changes are as important as the material solutions with which we desire to fight and win. Intelligence policy considerations in multi-domain operations and large-scale combat operations should not be a top-down effort. The real impetus for change will come from intelligence Soldiers and their leaders—those who need us to adjust our stance so that they can compete and operate in conflict, denying our adversaries any advantage.

Endnotes

1. *Merriam-Webster*, s.v. "policy (n)," accessed 15 April 2019, https://www.merriam-webster.com/dictionary/policy.

2. Irving L. Janis, *Crucial Decisions: Leadership in Policymaking and Crisis Management* (New York: The Free Press, 1989), 235-236.

3. Janet A. McDonnell, "The Office of the Under Secretary of Defense for Intelligence: The First 10 Years," *Studies in Intelligence* 58, no.1 (March 2014): 13.

4. "Frozen Conflict," Wikipedia Foundation, last modified 12 April 2019, 07:20, https://en.wikipedia.org/wiki/Frozen_conflict.

5. "Interior lines," Wikipedia Foundation, last modified 2 November 2018, 08:49, https://en.wikipedia.org/wiki/Interior_lines.

6. Jared Serbu, "Military readiness problems can't be fixed overnight, Defense chiefs warn," *Federal News Network,* February 8, 2017, https://federalnewsnetwork.com/defense/2017/02/military-readiness-problems-cant-fixed-overnight-defense-chiefs-warn/.

7. Chairman of the Joint Chiefs of Staff Manual 5230.01A, *Joint Staff Foreign Disclosure and Foreign Visits Programs*, 21 December 2017, A-2.

8. Ray Finch, "The Tenth Man–Russia's Era Military Innovation Technopark," *Mad Scientist Laboratory* (blog), August 20, 2018, https://madsciblog.tradoc.army.mil/tag/pacing-threat/.

Mr. Gregory Hatter is the Headquarters, Department of the Army (HQDA) G-2's Foreign Disclosure Policy Officer. He has been in his current position since 2001.

Mr. Scott Schultz is the HQDA G-2's Chief of Foreign Disclosure.

Mr. Craig Bell, a retired Army military intelligence officer, is the HQDA G-2's Foreign Language Team Chief.

COL Lisa Walker, an Army military intelligence officer, serves as the HQDA G-2's Military Deputy to the Army G-2X.

COL Bill Mangan, an Army military intelligence officer, is the HQDA G-2's Deputy for Plans and Integration.