International Law Studies - Volume 83
Global Legal Challenges:
Command of the Commons, Strategic Communications, and Natural Disasters
Michael D. Carsten (Editor)

III

Global Commons and the Role for Intelligence

Lowell E. Jacoby*

Introduction

This article attempts to answer four questions concerning the global commons and the role for intelligence in the evolving circumstances in which transnational terrorism has replaced the military capabilities of a small set of potential adversarial States to become the primary threat to the United States and its interests. First, how broadly should the global commons be conceived (space, air, surface, subsurface, seabed, cyberspace)? Second, what are the primary threats emanating from the global commons? Third, what role should elements of the intelligence community play? How will they be integrated into a plan for command of the commons? Finally, the Chief of Naval Operations and the *National Strategy to Achieve Maritime Domain Awareness*[1] call for a persistent intelligence, surveillance, and reconnaissance (ISR) capability in the global maritime commons. What obstacles will we face in achieving that? Are any of those obstacles legal ones?

Domains of the Global Commons

In a more rule-driven time, one or more of the space, air, surface, subsurface, seabed and cyberspace domains might be excluded from the commons. Concepts such as sovereignty, control of airspace or the seas, nation-State identity and prerogatives,

* Vice Admiral, United States Navy (Ret.)

and territorial waters had great meaning. Much of the meaning of those concepts and many of the accompanying rules are obsolete.

What forces have changed this situation? Globalization, the information age, the threats of terrorism and weapons proliferation are some of the factors at work, along with associated concerns over narcotics trafficking, smuggling and movements of illegal aliens, just to name a few.

The threats have redefined the commons. We speak of "ungoverned spaces" such as Somalia, or portions of nation-States where the government does not have effective control, which is a relatively common occurrence in today's world. These areas are part of the global commons. They become potential havens for terrorists, or the source of other threatening activities. In the past, when nation-States lost control of some of their territory it was typically of concern to that State and maybe to its neighbors. Today, these situations are of far broader concern because of their association with the global commons.

The information age has had a tremendous effect. Cyberspace is a difficult-to-define, but an absolutely essential element of the global commons with great potential for both good and evil. It's a largely ungoverned space apparently devoid of strong international conventions, an extensive body of legal opinion and precedence, and effective enforcement mechanisms. The debate within the United States over domestic surveillance is a manifestation of the issues concerning cyberspace and its position as the nexus of the commons and threats in the information age.

The components of the global commons are interconnected, interdependent and mutually reinforcing, making the associated issues very complex. Consider the following illustrative example. The threat is terrorist use of weapons of mass destruction (WMD) and the coordination of the planned operations occur over the Internet using advanced commercial technologies combined with use of multiple obscure dialects by a security conscious group with haven in ungoverned space. The movement of associated personnel is through established smuggling routes, the transportation of components for the weapon is facilitated by a narcotics network and the final movement of WMD to the planned attack location takes advantage of containers embedded in legitimate maritime trade. When viewed in this context, both the scope of the problem, and the need to master the global commons situation, come into focus. This scenario also captures the difficulties attached to the intelligence problem—a problem of scale, scope, complexity and the challenges presented by a highly accomplished foe.

The Primary Threats

Two conditions must exist for a threat to exist. An entity must have both the capability and intent to do harm.

The primary concerns are terrorism and proliferation of weapons of mass destruction. The worst case situation is the one where the two interconnect and terrorist groups with broad reach possess WMD attack capabilities. In this situation, capabilities and intent combine to present a threat of major proportions.

The global commons may play a key role in this threat scenario. The challenge for intelligence is to present the information required by decision makers that will enable them to defeat this threat. It is an awesome challenge and responsibility.

It is important to realize that a broad range of challenges to stability, economic well-being, international commerce, health and welfare also originate or can be abetted by employing the commons. Again, the intelligence challenges are immense.

Finally, there's an additional capability that deserves great attention, and that is the capability to disrupt or destroy the ability to communicate and access the data that's the lifeblood of today's world and modern military capabilities. Major disruption or destruction of these capabilities could threaten the global economy.

The Role and Integration of the Intelligence Community

Command of the commons is not a realistic goal, if the global commons are broadly defined. The ability of the adversary to hide and disguise activities, the limited value of traditional techniques such as deterrence and dissuasion, the pace of globalization and information technology changes, the interconnected nature of the problems, combine to make the concept of command of the commons in the traditional sense of command of the sea unachievable.

I take this position based upon what I believe is a realistic appreciation of what intelligence can achieve. If we attempt to know everything about everything all the time, which is what command of the commons would entail, we will fail. The result will be that we know some things about some things all the time and we will have spread ourselves too thin to be effective in providing requisite knowledge to decision makers. Rather, the key is to focus our efforts and dominate those portions of the commons that are integral to our priority objectives.

The key is to be selective and to prioritize our needs. Rather than control of the commons, we should focus efforts on achieving domination of those portions of the commons that are important at a specific time and place. This is akin to what is typically done in counter-narcotics interdiction operations. Intelligence collection

and analysis, plus the operating forces, are focused on a specified area for a specified period of time. This focus is overlaid on a fundamental understanding of the problem and operating patterns which has been achieved over time.

Intelligence must be agile and responsive to changing circumstances and decision makers priorities in this expansive common space. That requires intelligence to simultaneously provide breadth and depth. Breadth provides the foundation for the effort. It allows intelligence professionals to know something about everything all the time. This breadth then enables the focused efforts needed to employ capabilities and to inform decision makers as priorities are established.

Intelligence needs to be an integral part of the plan. The plan must establish priorities. It is essential that intelligence planners work with operators and decision makers to ensure that the intelligence capabilities are resourced and that the expectations are realistic. The resultant intelligence plan needs to be an integral part of the overall plan. And, as unforeseen circumstances are encountered, the agility and responsiveness based upon intelligence breadth and depth will be tested. A key element is that intelligence capabilities need to be in place early. They cannot be created after the priorities change. By then it is too late.

Finally, intelligence capabilities must span from unclassified data that is available in the public domain to highly sensitive data collected by highly classified means. These capabilities must encompass the data and expertise that friends and allies can contribute to assist in solving these very difficult problems. The data must be presented using the most modern information management techniques available and must reside on protected networks that employ the most advanced tools and capabilities. And, since the output of the processes is knowledge, the data must be processed through the minds of highly talented, dedicated and trained men and women.

A Persistent ISR Capability

Persistent surveillance is the capability to linger on a specified problem for as long as it takes to fully understand the issue or solve the problem. The problem may be to track an individual ship. The problem may be to monitor activities in a specified port. The problem may be to understand the activities of a particular shipping company that is potentially involved in illicit activities. The problem may be to understand the intentions of a specific individual. The problem may come down to identifying and tracking a single container that is in intermodal international commerce. Obviously, these and other problems that are encountered are great in terms of magnitude and complexity. It really is the issue of finding, and then maintaining contact on that often-discussed needle in the haystack.

The solutions to the problems will come from a variety of sources ranging from satellites in space, to human intelligence collectors, to examination of legal documents and financial records, to whatever sources of information may contribute to solving the problem. Tracking that container, for example, requires a great deal of international cooperation. The goal is to identify and begin the tracking at the point of departure so it can be interdicted at the optimal point during its movement. Once the target enters that intermodal transportation system, the surveillance problem becomes very, very difficult.

There will be legal issues threaded throughout. I have great appreciation for the close partnership that must exist between intelligence professionals and legal counsel. That partnership must be in place throughout the intelligence process. It must begin with the development of the plan and continue throughout the operation. That partnership needs to part of the overall plan. It can't be attached at the end if it is to be effective.

Conclusion

The concept of global commons must be very broadly defined and encompass the domains of space, air, surface, subsurface, sea beds and cyberspace if it is to be a useful construct in this era of globalization, rapid information age advancements, and the threats of terrorism and proliferation of weapons of mass destruction. The domains of the global commons are interconnected, interdependent and mutually reinforcing.

The capabilities of the US intelligence community, and those of friends and allies, are integral to efforts to dominate the global commons. These intelligence capabilities must be simultaneously broad and deep. Intelligence required to successfully operate in the global commons will be derived through a broad variety of sources from unclassified data that is publicly available to highly sensitive data collected by highly classified means. The most modern information management techniques must be applied to the data and the data must reside on secure networks employing the most modern tools and capabilities.

Key to dominance in the global maritime commons will be an ability to provide persistent surveillance. Persistent surveillance in the global maritime commons will be achieved by fully integrating a broad variety of information sources into a coherent, agile capability that allows analysts to generate the knowledge needed to make informed decisions with respect to the global maritime commons.

The expanse and complexity of the global commons presents problems of scale, scope and a convenient operating space for highly accomplished, sophisticated and dedicated foes. Only by recognizing the broad expanse of the commons and

focusing our intelligence efforts on those portions that can yield the information necessary to counter the wide array of threats can we address the new and emerging security challenges of the twenty-first century.

Notes

1. Department of Homeland Security, National Strategy to Achieve Maritime Domain Awareness (Oct., 2005), *available at* http://www.dhs.gov/xlibrary/assets/HSPD_MDAPlan.pdf.