Private Enterprise Intelligence: Its Potential Contribution to National Security

ROBERT DAVID STEELE

LOSING OUR WAY

Too often the intelligence community forgets its roots and abandons its private sector allies. Spies existed before Christ, but most of them were actually legal travelers and discreet merchants. Tea was stolen from China, and porcelain from England, by merchants.[1] More recently Japan, China, and Taipei have demonstrated profitable and cost-effective private intelligence capabilities. France and Israel excel at government support to the private sector, but it is possible that soon the private sector will be conducting most of the espionage as well as the open source intelligence (OSCINT) collection for these two countries and many others.

The Western intelligence communities lost their way in the late 1950s, largely because of over-reliance on the American intelligence budget as a safety net, with the unfortunate result that the American tendencies to ignore counter-intelligence and cultural intelligence, and to rely on technical panaceas and bean counting, infected the other services and skewed the manner in which US respective intelligence services trained, equipped, and organized for sustained warfare against 'the threat'.

Among the worst of the American influences on Western intelligence were its obsessive focus on the Soviet Union as the only enemy worthy of total attention, and an extremely expensive and deceptively ineffective technical collection empire,[2] which had the unanticipated impact of precluding American human intelligence (HUMINT) from developing into a serious clandestine service. In the aftermath of World War II the Americans displayed their distressingly usual tendency to take the easy way, and had attempted to penetrate the Soviet Union using emigrés and others from organizations which had already been thoroughly penetrated by Soviet intelligence. When all of these 'agents' were captured and executed, rather than doing some serious soul-searching and then creating a more serious illegals capability, the Americans turned to the U-2 and its follow-on satellites as an 'acceptable' alternative to traditional spycraft. Now the US finds itself facing a wide range of threats which are not amenable to technical penetration, while being simultaneously handicapped by the absence of a clandestine service worthy of the name. A side effect of the American dependence upon imagery intelligence (IMINT)

"Private Enterprise Intelligence: Its Potential Contribution to National Security," in *Intelligence and National Security* (1996)

and signals intelligence (SIGINT) overhead collection systems was the abandonment of the robust, diverse, responsive, and relatively inexpensive capabilities of the private sector.

It is instructive, in thinking back to the early days of the Office of Strategic Services (OSS), to consider how very important the academics from the private sector were to the development of our analysis methods, and how very important open sources were to American strategic intelligence efforts.[3] Miles Copeland has described how the OSS handled the innumerable requests from the Department of State and the Pentagon which did not merit clandestine collection. The OSS put two men in a room with *The New York Times*. Anything that could be answered from this open source was typed up, stamped secret, and disseminated as the purported result of a highly compartmented human intelligence operation – and one which was ostensibly very expensive, hence justifying requests for additional funds. The information itself was not fabricated, only the purported methods of acquiring it.[4]

OSCINT has maintained a modest role within the larger intelligence communities, and a more central role within the smaller intelligence communities, but the reality is that the Anglo-Saxon intelligence communities of today exploit less than 10 per cent of what is available from the private sector. The aim of this essay is to explore the larger strategic context within which private enterprise intelligence can make a contribution to national security; to understand operational concepts from private enterprise intelligence which can and should be adopted by the traditional government intelligence services; and finally, to make an inventory of some of the specific private enterprise intelligence capabilities which can be used by the government to achieve both tactical results and sustained savings.

OSCINT AND THE CHANGING THREAT

Other essays in this collection address the changing threat and changing intelligence agenda, but I wish to outline here an intellectual construct which influenced my early appreciation of how poorly the US intelligence community exploits private sector intelligence capabilities, and how relevant OSCINT is to the threats that have always been with us, but which are receiving a more appropriate degree of attention today.

While there are obviously variations to these four categories, they helped me focus on the original threat – the high tech brute (conventional military opponent) – while also keeping sight of the three major emerging threat categories. This matrix bears on two fundamental aspects of national security and national intelligence. First, since the National

FIGURE 1
THE FOUR WARRIOR CLASSES AND IMPLIED INTELLIGENCE CHALLENGES[5]

		GUERRILLA WARS		
Physical Stealth, Precision Targeting	HIGH TECH BRUTES (MIC/HIC)		LOW TECH BRUTES (LIC)	Natural Stealth, Random Targeting
		Money – Ruthlessness		
ECONOMIC WAR		Power Base		TERRORISM
		Knowledge – Ideology		
Cyber-Stealth, Database Targeting	HIGH TECH SEERS (C3I WAR)	CULTURAL WARS	LOW TECH SEERS (JIHAD)	Ideo-Stealth, Mass Targeting

Security Act of 1947 which created the US intelligence community, all that has followed has led to an intelligence community trained, equipped, and organized to deal with a single monolithic 'high-tech brute', the Soviet Union, and very poorly trained, equipped, and organized to deal with smaller high-tech brutes, such as Iraq, or the other three major categories of threat. In particular, national intelligence capabilities in support of both international and domestic law enforcement, and economic competitiveness, are mediocre to non-existent.[6] The US intelligence community does not have the long-term ethnic human penetrations it needs against international criminal or terrorist organizations, nor does it possess the kind of tactical SIGINT capabilities, or even air-breathing tactical IMINT, that would be helpful in coping with these challenging international threats.[7] Cultural movements baffle 'Western' technical indications & warning (I&W) systems because they do not use point to point communications but rely instead on couriers, the pulpit, and broadcast television indirectly to mobilize action elements from within the masses.[8] The US does not have an electronic counter-intelligence capability worthy of the name, nor has it established the most basic economic counter-intelligence capabilities.[9] In short, *Our intelligence communities are not ready to deal with three of the four warrior classes!*[10]

Second, it is clear that OSCINT can meet the vast majority of America's intelligence needed against the emerging threats, and that OSCINT must be the foundation upon which we completely restructure our classified capabilities. While serving as the senior civilian responsible for the establishment of a new $20 million intelligence production center, the US Marine Corps Intelligence Center, I was shocked to discover that