The Foreign Policy Impact of Privatized Intelligence

https://www.e-ir.info/2011/08/15/the-foreign-policy-impact-of-privatized-intelligence/

ANDREW BROWN, AUG 15 2011

What does it mean when corporations begin to take on the tools and capabilities formerly reserved to large states? The use of private military forces such as Blackwater has been well documented and now we find an even more interesting trend in the global corporate world. Companies developing in house or utilizing contract private intelligence groups to spy on their competition and more disturbingly to conduct deniable direct attacks against their physical infrastructure and computer systems. This is a growing concern not just for the business world but for the core national interests of states around the world.

Private intelligence use in corporate affairs begins with the state. Many nations developed corporate espionage capabilities over the past fifty years to support their domestic economies. Companies in countries like France, Korea, Japan and Russia were supplied with valuable commercial intelligence in order to better compete with their international rivals. Some nations, like Japan, have shaped virtually their entire overseas intelligence apparatus around developing commercially, as opposed to strategically, valuable intelligence. The peak of state intelligence support for corporate concerns was in the 1980's. With the end of the Cold War large numbers of states began a drawdown of their expensive covert intelligence networks overseas. The legacy of this is twofold. First, companies were no longer being provided the commercial intelligence that they had come to rely on from the state. This has lead to the explosive growth of a private intelligence sector. The second factor at play has been the waves of unemployed spies which have flooded the private sector beginning with those from the former Soviet Union and Communist bloc countries and today growing even more rapidly thanks to an influx from Western intelligence agencies due to the end of the global war on terror and the better pay in private sector intelligence. This expanding talent pool has fueled the growth of private intelligence as former state spies became widely, and relatively cheaply, available to companies around the world.

The impact of private intelligence is being felt throughout the global business world as company after company is attacked by trained and case hardened spies working for rival concerns. No country is immune to the economic hemorrhaging that can occur when their companies are routinely penetrated by foreign competitors. This can best be seen in the United States where economic espionage annually costs American companies more than 100 billion dollars in lost business, stolen technology and the consequences of direct attacks. This is a tremendous amount of money and has already deformed a number of segments in the US economy, particularly the banking and investment sectors. The dramatic loss of competitive advantage and technology to overseas companies is having an impact on the US business community which is almost totally ignored by government counter intelligence and political groups. Were the US government to begin a crackdown on corporate espionage from overseas it would have a significant impact on relations with a number of allied nations and competitor states like China. More attention to this issue may well be in the works as the US begins to wind down its efforts targeting radical Islamist elements in a post-Bin Laden world. The intelligence and defense communities need a very good reason to continue to receive the massive post-9/11 budgets in this era of belt tightening and corporate espionage makes for a very seductive target. This is particularly the case as modern private corporate intelligence groups begin to utilize more advanced cyber weapons to directly and deniably attack companies at the behest of their rivals. There have been a number of very well publicized cases of this in recent months and this trend has nowhere to go but up.

The use of advanced cyber weapons to spy on and directly attack national as well as rival corporate systems is already an issue in the media and among foreign policy experts. As private intelligence grows and becomes solidified

within the international business world pressure on leaders and governments to address this issue will increase. These weapons are becoming extremely powerful and their consequence free use by private intelligence groups on behalf of their corporate backers has already lead to massive financial losses in multiple countries. The main point here is that corporations have limited liability under international law and are far less vulnerable to detection and thus sanction than nation states. While the use of advanced cyber weapons by states will almost certainly be classified as comparable to physical attack and thus deterred the private use of such weapons holds little risk when carried out covertly. The tail (corporations) are going to wag the dog (the state) when it comes to 21st century private intelligence use as economic competition between states increases and the capabilities of corporate spies improves. There is little regulation and fewer sanctions available to keep companies from adopting private intelligence as a core aspect of their competitive advantage. The disadvantages for companies that do not keep up with their competitors by developing a corporate intelligence capability are also growing each year.

America is the only industrialized power that does not use its state intelligence apparatus to steal commercially valuable information on behalf of its domestic companies. What is happening today is that many US based firms are awakening to the advantages that their overseas rivals have gained from intelligence and adopting these practices themselves to fight back. With no support from state intelligence agencies US businesses are developing and deploying covert intelligence and direct action capabilities with near zero oversight, or clandestine help, from the government. The potential for significant political and foreign policy blowback from this trend cannot be overstated. While the US government is more than happy to bury cases of corporate espionage against domestic firms in the name of good foreign relations other nations are by no means going to be act so conciliatorily when it comes to agents operating covertly overseas at the behest of US companies. This is also the case with US companies using cyber weapons to target their overseas, less well defended, rivals. As cyber war, and correspondingly cyber espionage and sabotage, becomes more of a global issue in the 21st century its use by both American firms overseas and foreign firms in America is going to have a place at the foreign policy table. The longer an adequate system of norms takes to be implemented and accepted the more contentious this issue will become.

Andrew Brown *is the author of the recently released book The Grey Line: Modern Corporate Espionage and Counterintelligence.*