Economic Espionage: The Curse of ‘Soft Spying’

Despite Hollywood romanticizing about Bonds and Bournes, one of the most prevalent forms of modern intelligence activity is also arguably the least emphasized: economic and industrial espionage. Aimed at garnering a financial and innovation advantage for countries seeking greater influence in a highly globalized world, this activity is not just about economic policy but serves as de facto proxy military rivalry: states maneuver to outperform, outwit, and ‘outstrategize’ across all spheres of profitable activity via this lesser ‘intelligences’ activity.

The motivation to engage in soft spying and conduct economic espionage is no small matter. The end of the Cold War signaled a shift from heavy emphasis on military alliances to the focus on hyper-economic development. It was not so much the end to war and cessation of hostile activities as a switch to competition with more productive and prosperous end goals. All around the world states understood that failure to keep up in a rapidly globalizing economy could likely doom a state not just to economic hardship but expose it to dangers of the decidedly old-school realist variety: war, occupation, loss of territory, and the like.

Emphasizing economic development, however, does not magically create an industrial juggernaut overnight. As soon as developing states began to realize just how difficult steady, progressive, rational growth would be, they began finding ways to shortcut the journey. Soft spying became arguably the chief method in this new national security priority of economic development. Spy movies notwithstanding, the traditional methods of economic espionage truly read like a primer from Ian Fleming: planting moles and/or recruiting inside agents; surveillance; clandestine entry; bag drops and collections; dumpster diving; bugging and phone tapping; invasive computer programs; and drop-by spies.

The act of American businesses trying to steal secrets from other American businesses is considered a standard part of the game, if perhaps a distasteful one. It is not explicitly illegal when competitors strive to gain early access to patents, trade secrets, strategies, and the like. The domestic laws of many states, America included, do not explicitly prohibit intruding into foreign lands for the direct purpose of acquiring and collecting economic information. This might be part of the motivation behind why so many American businesses tend to avoid preaching about the elimination of soft spying and why such espionage activity is often ignored when done by traditional allies.

So while soft spying can technically be framed by some proponents of international law as a violation of sovereignty and the principles of non-intervention, the empirical problem remains that hardly any states take such claims seriously. Thus victim states more often than not find themselves arguing in the dark, as there has not been any success in establishing a global business culture that treats economic cyber espionage as the same thing as more traditional prohibited forms of force and invasion. International groups like the World Trade Organization (WTO) - a body that should have a natural alignment in seeing greater progress against soft spying – has to date shown no major prioritization or interest in this objective. This is yet another case where the structural rules governing the system hinder progress: in the WTO context, it is difficult trying to establish economic espionage as actually violating any specific or explicit WTO agreements. The WTO, just like international law, establishes guidelines for members’ operations inside their own territories. There are no established procedures for imposing punishment or enforcing such guidelines outside of those limits.
There is yet another double-dilemma in the international sphere: there are no rules currently that prevent American companies from corrupt or improper business practices overseas. The United States has attempted to self-regulate with the passage of the Foreign Corrupt Practices Act, but even with this effort there is a fundamental structural problem with the global system: very few nations have enacted laws criminalizing the bribing of foreign officials in terms of economic commercial activity. This is not so much because only America cares about corruption or doesn’t ever engage in economic information collection on its own. Rather, it is a testimony to how prevalent the focus is with the rest of the world on developing at any cost.

Speaking bluntly, the position of dominance occupied by the United States in terms of technical innovation and corporate long-term strategizing makes nearly every other country in the world lesser in comparison. It is not so much about how ‘provable’ this is with data as it is about the ‘perception:’ most of the world’s countries believe it has little to offer America in terms of intellectual and industrial property worth stealing (at least in comparison to what foreign countries think is worth stealing from the United States). Paradoxically in terms of soft spying, this perception is actively encouraged on the American side, as evidenced by former CIA director James Woolsey, who infamously stated that there were only a few areas of European technology that surpassed American versions, but that those areas were ‘very, very, very small.’ As such, the concern for adopting explicit, enforceable and transparent legal rules to constrain soft spying remains infantile and largely undeveloped, even in the primary victim nation of the United States.

In totality, it is obvious that the United States accepts and understands the gravity of economic espionage and its cascade effects that go far beyond industrial profiteering. What America has not been able to do is enact effective legislation that gives governmental agencies the proper freedom and jurisdiction to intervene in or change a business culture that seeks to ‘handle its own affairs’ without any governmental intrusion. Not only does American industry at times handcuff the government and its own security organizations from properly protecting crucial assets, and often does so with an overly cavalier attitude that feigns hyper-vigilance and competence, it appears previous discussions that considered the possibility of American intelligence proactively ‘helping’ American businesses were also deterred by design. This arguably leaves the United States even further exposed and weak in comparison to other countries that have no qualms about using their own intelligence communities for such activity.

If there is general wariness between business and government, then it is hard to understate the mistrust and near derision expressed when business community leaders are asked if formal American intelligence agencies should proactively engage in economic espionage for the benefit of American industry. Direct cooperation and interaction with the American Intelligence Community is seen as something anathema to best business practices and somehow a violation of business ethics. It is not so much that the United States does not collect economic information from foreign sources. America does not deny spying on foreign firms and business interests. But it does deny that such spying goes on for a particular industrial purpose or for the advancement of specific American industries so that they may be more competitive in the global market. Whether one wishes to believe that position fully or offer exceptions to that general rule, it still results in the United States being in a surprisingly ignorant and dangerous position.

Dr. Matthew Crosston is Professor of Political Science and Director of the International Security and Intelligence Studies program at Bellevue University, exclusively for the online magazine “New Eastern Outlook”