The company-intelligence interface: Government policy, corporate expectations, competing futures

Mikhail Koulikov

Available at: https://works.bepress.com/mikhail_koulikov/22/
Traditionally, the terminology of information-gathering and information analysis activities has varied based on who is performing them, and to what ends. Concept like ‘market research’, ‘business intelligence’, ‘competitive intelligence’ and ‘industrial espionage’ each imply different actors, different skill sets, and different processes. Yet the overarching goal of all of these activities is the same: to find out that which you do not know, and to protect your own knowledge, or even ‘meaningful information, if one takes Winkler’s (2005) idea of the relationship between information and knowledge, from your adversaries. And if the goal of all of these activities is the same, the specific roles of the people who perform them becomes a valid question for discussion and debate. In the last several decades, this question has been asked and answered in different ways in various countries around the world. In the U.S., however, it is only within the last fifteen or so years that it has truly come to the forefront. But in these years since the end of the Cold War, the role of the government in providing intelligence and counter-intelligence support to private business has been a hotly-contested issues across the realms of political science, law, and business ethics. With the announcement earlier this year of the current U.S. National Counterintelligence Strategy, which specifically calls upon the Intelligence Community to “protect economic advantage, trade secrets and know how” (Office of the National Counterintelligence Executive, 2007), it appears that at least on the policy side, this issue has been resolved. But of course, the follow-up question that has to be raised asks what this kind of policy means for American companies of all shapes and sizes in the modern globalized economy. To answer this question, it will be important to look at the history of government
involvement in economic intelligence throughout the history of the U.S. Particular attention will have to be paid to evolution of the debate on what Trim (2000) calls the “company-intelligence interface” from 1991 on. And to make this assessment something more than just a literature review, the next step would be a strategic analysis this looks at the political, social, economic and technological implications of this debate. Nor would it make any sense to merely stop at the point when a policy that aligns the interest of government intelligence agencies and the business world was generated. Conditions change; policies evolve to reflect changes, and the final question is always not “where are we?” but rather, “where are we going?”

The first American intelligence-gathering entity, the Committee of Secret Correspondence, was founded even before the Declaration of Independence. One of the Committee’s first acts was to dispatch an agent to Europe, tasked with what in modern language would be called gathering of open-source economic intelligence on such topics as the European market for tobacco from America and elsewhere (Zelikow, 1997). As the intelligence community evolved and developed an institutional structure throughout the 19th and early 20th century, the collection of economic intelligence in furthering America’s national interest was consistently recognized as a vital task. Similarly, economic espionage played a significant role in the early development of American industry; for example, as Fialka (1997) notes, the development of the New England textile industry was greatly aided by the illegal acquisition of a piece of English industrial technology (the Cartwright loom) by a private American individual. On the other hand, America’s economic counter-intelligence efforts generally – and not always successfully – focused on protecting products and processes with particular defense or national security applications (Friedman, 1998).
By 1949, economic intelligence duties were formalized within the CIA as the task of the Office of Research Reports, although almost immediately, tension developed between its activities and those of the State Department’s economic analysis functions, carried out primarily by the Bureau of Intelligence and Research. While initially, the CIA was involved largely with gathering macroeconomic data, as early as 1958, Helsper presented a set of recommendations for the “systematic study of industry at the corporate level”, primarily by analyzing published annual reports. It was also not long before the first controversies arose surrounding the involvement of the CIA in gathering commercial intelligence or acting for the benefit of American businesses. Turner (2005) points out the danger of explicitly or implicitly giving one company advantage over another. He also notes that both at that point and later in the history of the CIA, the idea that the economic well-being of American companies and the actual national security of the country are closely related was simply not yet accepted. For example, Fort (1993) notes a CIA agent saying that he is “prepared to give my life for my country, but not for a company” to the then-current Director of Central Intelligence.

Throughout the first four decades of its existence, the primary activities of the Central Intelligence Agency were directed against the Soviet Union (DeConcini, 1994). The collapse of the USSR, brought about a period of looking inward, of identifying new missions and new objectives, and of intensive debate about the kinds of tasks the CIA should perform. Intelligence activities in support of business goals were by far not the only new task that was discussed, but the variety of perspectives on it was extremely wide-ranging. As early as the fall of 1991, Turner argued forcefully that the post-Cold War reality would call for a “more symbiotic relationship
between the worlds of intelligence and business” as one of three major new directions in U.S. intelligence policy. He again recognized the many specific issues that would arise from the involvement of the U.S. government in economic espionage for the benefit of particular companies, such as the potential for tension with friendly governments and the difficulty of determining national allegiances of international or multinational corporations. At least at that point, Turner chooses to “pass the buck” by involving other government agencies, such as the Commerce Department, in making some of these decisions. Wright (1991) also acknowledges the “moral, political and practical” concerns that arise from affirmatively answering whether or not the U.S. government should “assist business activities in competing for foreign markets.” Some of the arguments he proposes include the idea that a ‘level playing field’ in international economic competition is basically a myth, and that there is no reason for the U.S. not to do what dozens of other countries are doing already. In the same essay, he introduces to the intelligence community the idea that shifts in the world economy, on the level of the industry, the country and the region all have particular implications for national security. He cautions, however, that any kind of government involvement in business intelligence will only be truly successful if the underlying idea of any such efforts is equal or at least equitable assistance to “all U.S. commercial and business activities overseas,” regardless of company size or other factors.

Of course, critiques of these kinds of proposals were not far behind. Kober (1992) structured his thoughts around asking first whether American economic dominance can ever be threatened enough to make economics a matter of national security. The second part of his argument raises the point that the CIA is simply not designed for economic intelligence-gathering and that the skill sets of its analysts are woefully inadequate for this area. He also particularly highlighted the
potential for corruption, bias, and abuse of an intelligence-company relationship via lobbying and influence-peddling. Kober’s view finds support in a New York Times article (Sanger & Weiner, 1995) which quotes a senior CIA official’s lament that the country’s top economics graduate students are highly unlikely to commit to intelligence analysis careers, especially when private-sector opportunities are so plentiful. His later (1996) follow-up paper on this topic links a critique of any government involvement in business intelligence to a more general argument against protectionism and neo-mercantilism.

Throughout the early and mid-1990’s a number of other leading policy-makers and political scientists introduced their own approaches to the debate. In his 1994 article, Dennis DeConcini, at that time a U.S. Senator and the chairman of the Select Committee on Intelligence, noted that the business world itself was not enthusiastic about assistance from the U.S. intelligence community, primarily because of reasons of cost and the low possibility of gaining access to highly specific information tailored to the needs of individual firms, rather than raw, unprocessed data. On the other hand, he argues for an increased role for the intelligence community in enforcing existing trade agreements. Finally, he introduces the possibility of using intelligence assets to establish an open clearinghouse of foreign commercial information. An initially appealing concept, even this raises issues of whether there are other entities within the U.S. government that are better suited to this role, A secondary problem he identifies is the same one that was noted by Turner (1991): how to limit access to American companies and interests only, in an age of international partnerships and global ownership. DeConcini’s specific guidelines for future policy include a strong recommendation that the intelligence community “not attempt to satisfy private requirements,” while cooperating with the Department of Commerce, Department
of State, and Office of the U.S. Trade Representative as appropriate to promote competitiveness on a nationwide level. He also emphasized that the intelligence community should not yield to the temptation of “obtaining and disseminating publically available information.” However, his paper does note that intelligence agencies do have a significant role to play in economic counter-intelligence. It calls for a “new criminal statute” that would address economic espionage and apply not only to classified or sensitive information, but also to trade secrets. DeConcini’s proposal indeed served as one of the sources of what became the 1996 Economic Espionage Act, which explicitly the theft of trade secrets an explicit criminal offense.

More thinking about this relationship came from the intelligence community itself. Burton (1994), writing in the unclassified section of the CIA’s Studies in Intelligence journal focused on the limited cost-effectiveness of government commercial spying. “The additional money spent on…intelligence collection might produce better results if it were spent on improvements in education, research and development,” he argues. Burton’s radical solution to the issue was to propose international agreements between the U.S. and other countries that would codify keeping intelligence agencies out of the commercial realm. Evans (1994) reminded there is an important difference between “macroeconomic espionage” – long an accepted task of the Intelligence Community; economic counterespionage; and microeconomic espionage. The areas in which he proposes the Intelligence Community can meaningfully serve private business include translation, for example of published budgets of foreign government entities that are involved in business activities and more general compilation of “foreign industrial policies” based on open-source materials. Kristen Michal (1994) looked specifically at the role of the intelligence community in assuring business counter-intelligence. Her thinking is that a better allocation of
the resources of the intelligence and law-enforcement community would be to educate the
corporate world about espionage and counter-espionage, while at the same time asking
policymakers to concentrate on “increasing the costs of committing economic espionage in the
U.S.” – again a recommendation that found its reflection in the Economic Espionage Act. The
same kind of suggestion is given by Schweizer (1996), who notes that while the early 1990’s saw
the U.S. intelligence community begin engaging in “identifying unfair trade practices and
industrial espionage,” in many cases, those efforts were awkward at best. He proposes that rather
than jumping into the economic espionage quagmire, the better option for the U.S. would be
vigorous law enforcement coupled with “greater diplomatic fortitude” in responding to economic
espionage.

Soon after the adoption of the Act, the FBI’s Edwin Fraumann (1997) wrote in Public
Administration Review about the need to move beyond thinking of the CIA as the only agency
involved in economic intelligence and counter-intelligence. He placed the primary responsibility
for protection against economic espionage solidly on individuals and companies, while also
calling for continuing “cooperation and coordination between various government agencies and
the private sector,” such as via the FBI’s Awareness of National Security and Response program,
which briefs staff of private companies on potential espionage and business intelligence threats.
Fraumann also highlighted the role of the State Department’s Overseas Security Advisory
Council in providing both general consulting services and specific assistance to American
companies in facing foreign security threats. As mentioned earlier, one of the major questions
corollary to whether the U.S. government should collected and provide economic intelligence to
companies is whether it even can do so effectively. It is explored most fully by Russell in a 1994
paper prepared for the U.S. Army’s Command and General Staff College. In her view, the CIA
and NSA definitely possess the capability to collect and analyze economic intelligence. Actual
dissemination to the American business community, on the other hand, would be difficult to
implement, and would potentially require the involvement of other government agencies outside
the intelligence community. Porteous (1995), bringing to the discussion an outsider’s perspective
but a deep familiarity with the intelligence community, mentions that the lack of communication
between economic intelligence providers and their potential customers, both inside and outside
the government will continue to remain a major issue. He particularly notes that traditionally,
intelligence analysts have worked to provide answers to specific requests from specific
individuals, rather than predicting potential requests. Finally, Hancock’s (1996) approach to the
debate calls for establishing a set of guidelines for acceptable or permitted commercial
intelligence activities for the U.S. intelligence community. He argues that the existence of such a
framework would be particularly beneficial for the evolution of an international standard of
business intelligence practices Hancock also calls for the establishment of an “organizational
center” to guide various government entities in their commercial intelligence initiatives, in
particular to avoid duplication of activities.

At the same time as the intelligence literature was concerned with issues of implementation, a
separate group of scholars addressed the legal and moral angle of the same question. While
Russell, for example, specifically avoided discussing the legality of the intelligence-corporate
interface, this same topic is the focus of Augustini’s (1995) examination. He argues that while
both the 1947 National Security Act and Executive Order 12333, which establishes the rules for
collection and dissemination of intelligence information do not in of themselves prohibit the
intelligence community from engaging in economic intelligence tasks, they may prohibit dissemination of economic intelligence outside the government. He also finds that such dissemination would not violate the provisions of the Sherman Antitrust Act, but receiving such information may come into conflict with state-level intellectual property law. Augustini concludes by arguing that any discussion of the specifics of involving the intelligence community in working for the benefit of American business is premature until the broader question of whether responding in kind to economic espionage has been answered effectively. Perry’s (1995) consideration of the ethics of this kind of involvement is not able to endorse “deceptive and coercive intelligence methods” in the service of anything other than national security. He does, though, make a distinction between business intelligence and counter-intelligence, and accepts the involvement of the intelligence community in the latter. Pratap Chattergee, for his part (1996), is deeply skeptical of the entire idea of embracing economic espionage and counter-espionage as a new mission of America’s intelligence agencies; he argues that it is not much more than a ploy for finding “finding new public rationales for [the CIA’s] existence.” In an issue of Social Text, media scholar Richard Maxwell (1998) explicitly places the entire issue into the concept of the “Cold War II,” a condition where “interalliance economic spying no longer enjoys benign neglect in the name of a greater good.” In Maxwell’s view, economic espionage is not a symptom of the end of the first Cold War as much as it is an inherent feature of it; as a target, the U.S. is merely reaping what it has sown.

Another component of his view also attributed some of the debate to the maturation of the academic field of market research and its evolution into competitive intelligence. And indeed, while the intelligence literature tended to ask how agencies like the CIA could best serve the
needs of business, and the humanities literature wondered why should they, the emerging competitive intelligence profession began its own approach to the same topic. In a 1994 article, Herring states quite bluntly that the government is obligated to use legal means to aid the competitiveness of American companies. Acknowledging the debate, he then takes both sides of it to task for “talking past each other.” He blames business leaders who claim to not be interested in what the government can offer them for simply not having a solid understanding of the value of intelligence and counterintelligence, while also operating with extremely narrow views of what these terms mean. At the same time, Herring accuses the CIA and other parts of the intelligence community of not taking the time and effort to tailor their own offerings to the real or potential needs of a new and different clientele. The kind of government-corporate intelligence cooperation he proposes would involve first, education in what intelligence is and how it is best used, and second, facilitation of private-sector access to the sheer amount of open-source information that is collected by the intelligence community using entirely legitimate means. One task he specifically calls on the intelligence community to consider would involve a thoughtful evaluation of whether as much of the information that it collects but restricts from public availability should in fact be kept away from its most likely users. Supporting Herring’s assertion, Calof (1997) cites a study according to which, “76% of surveyed firms report they need better intelligence.” His paper calls on companies to develop a “North American CI [competitive intelligence] culture…” that would take into account “the need to have competitive intelligence linkages with other businesses, government, academe and associations.” A somewhat later (1999) paper by Calof and Skinner that is aimed at public-sector managers reminds readers that despite the stereotype, one of the greatest strengths of the intelligence community in the U.S. lies in its ability to gather open-source information, However, as noted
several times already, dissemination remains the weak point. And following Herring’s suggestion that education of the business community is a major pre-requisite to the establishment of a constructive relationship between corporate intelligence clients and government intelligence providers, several authors have since taken it upon themselves to clarify the difference between competitive intelligence and industrial espionage. Wright and Roy (1999) acknowledge that the distinction between the two is sometimes vague, but do note that the legality of methods are a major component of the definition. Moreover, according to them, competitive intelligence implies awareness not only of competitors, but also of suppliers and customers, as well as the “legal, technological and political” milieu within which any given company exists. This is, of course, not to say that the competitive intelligence literature is unanimous on the issue. Nolan (1994) recognizes the appeal of the involvement of the government in competitive intelligence, but is also of the belief that a lot of education needs to take place on both sides before any meaningful relationships between intelligence agencies and the commercial world can be established. Lisse (1999) arrives at the same conclusion, but also adds another ethical component by questioning the appropriateness of expending the taxpayer dollars of a government budget to further the economic interest of a corporation or private firm. He too takes the side of the issue that argues that because so much business information is available via open-source channels, there is actually very little value in the “more intrusive clandestine intelligence” that a government agency may instinctively perform. He does, nonetheless, recognize the role of the government in economic counter-intelligence. An extremely interesting approach is offered by Parker (2000). While most of the writing on this topic focuses on the links between major national companies and the intelligence community, he discusses the opportunities for “government competitive intelligence” (GCI) on the regional level. At this level, government
organizations possess many “unique competencies” that companies, and especially SME’s, may lack. Particularly important, according to Parker, is the ability of government employees to access existing networks and to build new ones. He also splits GCI initiatives into three types, aimed at other companies, entire industries, and other governments.

By the late 1990’s, after, it was looking like the debate on the role of the government in competitive intelligence had exhausted itself at least for the meanwhile. The Economic Espionage Act (EEA) went at least some distance towards reducing the perceived threat to U.S. companies from foreign firms, or at least provided them with a fairly obvious weapon, and arrests in the first case prosecuted under the EEA took place about a year later (U.S Department of Justice, 1997). And as it appeared that many of the practical issues around the relationship between government intelligence and business were put on hold, it is interesting to see where the next level of the evolution in theory took place. Joseph Bolick (1998) argued that “a nation needs economic power to act as a foundation and to support its other spheres of national power,” and went further by a second argument, that protecting the interests of American companies, even those that are not directly involved in defense-related industries, should in the interest of the American military and intelligence community. He proposed the establishment of an “information clearinghouse” tasked with the same kind of education and dissemination mission that was mentioned by Fraumann and Herring, but asks that the Department of Defense, in cooperation with other government agencies and, interestingly, not just individual companies but also “civilian business organizations,” take the lead in any initiative of this kind. The next year, in a paper published in the DOD’s Military Review journal, Bill Flynt (1999) issued what amounted to a wake-up call that named the threat from economic espionage as one of the major
challenges the entire U.S. community would have to face in the new century, alongside the threats from terrorists, hackers, “organized information warfare teams” and trans-national criminal organizations.

The most recent thinking about the proper intelligence and counter-intelligence role of the government and private companies is based not only on these ideas, but on the full range of opinions that have been expressed by the different participants in this debate. They answer some of the most difficult questions that have been posed, while also continuing to explore those aspects of the issue that had not yet been looked at in length. Loch Johnson (1999) advises the President to not hesitate to turn to the CIA to advance economic security and achieve economic objectives, especially in light of the development of entities like the National Economic Council. Trim (2000) argues, as I do, that the difference between corporate and government intelligence is of method, not goal. He also notes that no single agency, organization or entity has a monopoly on intelligence-gathering, and overall, bases his thinking on an idea of a “holistic approach to national security” that calls on increasing cooperation between government and industry as purely military methods of resolving international conflict become undesirable. One particular area of this overall question that had not seen a lot of discussion in the mid-1990’s, beyond the fairly biased writing of Kober (1992, 1996) had to do with the economic impact of government involvement in intelligence. This oversight was corrected by Jensen (2001). *Intelligence: An economic good* asks the producers of intelligence (within the government) to begin considering the actual cost of collecting intelligence, and to introduce the cost factor into how valuable intelligence is. He does not offer any specific recommendations, but nonetheless, the obvious implication of his paper is that if intelligence-gathering has a cost, it may be logical to expect it
to be borne by those it most directly benefits. Csurgai (1998, 2000) places competitive intelligence activities in the context of a shift away from inter-state relations to geopolitics and geoeconomics. In particular, he notes that a successful geo-economic strategy absolutely demands access to and manipulation of “huge quantities of information.” Clarke and Johnston (1998) examine the issue of the effect economic espionage and counter-espionage has on relations between countries that are otherwise friendly or even allied. They, however, argue that the costs of economic espionage are not likely to rise to such a point that it would not be tolerated in absolutely all cases, regardless of how it affects existing security relationships. Orton (2002) introduces the personal perspective of a business executive who is benefitting from alleged government intelligence-gathering assistance and shows how the mere perception of such ties frays existing business relationships and seriously challenges the concept of corporate social responsibility. Finally, Poteat (2006) reminds both business and intelligence that the stakes involved make economic intelligence-gathering and espionage much more than “ordinary theft of intellectual property.”

The most recent summary of foreign economic espionage in the US (Office of the National Counterintelligence Executive, 2006) notes that while government-sponsored economic espionage certainly occurs, the majority of foreign agents who engaged in espionage were not instructed or directed to do so by governments. As I have mentioned already, the current national policy on counter-intelligence endorses the idea that the government must do more to in support of the economic interests of private individuals and companies. The policy calls for collaboration between intelligence agencies, law-enforcement organizations and the business community in assessing and responding to economic espionage threats and calls for greater analysis of what
exactly represents the “vital national assets” of the United States. And in a very recent speech (2007), Joel Brenner, the National Counterintelligence Executive, focused precisely on what he calls an “antiquated” assumption that only companies performing classified or defense-related projects are worthy of counter-espionage protection and support. In the same speech, he notes that one of the effects of the current information age is that less and less information will in fact be secret as the speed of collection and dissemination continues to increase.

So, what does all of this mean – not for the intelligence community, but for companies that simply to not have the luxury of ever forgetting about their domestic and international competitors? The first thing that will be absolutely crucial to keep in mind will be that most likely, sooner or later, a company will have to deal with the realization that it is a target of economic espionage. Obviously, in some industries, this possibility is a lot more pronounced than in others, but a telling fact is that the first three defendants convicted under the Economic Espionage Act had been attempting to steal trade secrets from a manufacturer of mailing labels and other adhesive products (U.S. Department of Justice, 1997). The second is that the resources available to companies to counteract and combat economic espionage are a lot more extensive than one may initially think. Awareness of what economic espionage is and how it may be perpetrated is a necessity; an in-house counter-intelligence function is a luxury, and for many companies, plain-out not appropriate.

A political analysis of the current relationship between government intelligence/counter-intelligence and private business shows that for the immediate future, at least countering espionage against private business is considered to be an entirely appropriate mission for various
government agencies. The legal background, with the explicit criminalization of economic espionage, has underlined this, while the National Counterintelligence Policy resolves the debate within the intelligence community and reminds its members that their duties now go beyond supporting the traditional government customer. Since the current situation is the culmination of a vigorous debate that has taken place across three separate administrations, it is not likely that a major change will take place anywhere in the near future. One area in which there is not yet a lot of progress is the international status of economic espionage, whether from the standpoint of specific bilateral agreements between the U.S. and individual countries, or of broader treaties or policies adopted by regional bodies or even the United Nations. In fact, already, one major recent controversy has involved what a number of observers (Campbell, 2001; Schmid, 2001) believed to be an American intelligence-gathering system that tapped commercial communications in Europe for the potential benefit of U.S. corporate customers. Another issue that may be important is the fact that to date, sentences of persons convicted under the Economic Espionage Act have been quite light, leading some to argue that it is not a strong enough deterrent. On the other hand, there is very little in the way of political or policy support for enabling the American intelligence community to aid private companies in actually carrying out economic espionage in foreign countries. However, if the argument that economic intelligence and business knowledge are themselves vital national interests can be applied to the U.S., as it is, it stands to reason that the business knowledge of foreign companies represents the national interest of those countries. Acquiring this kind of business knowledge may be the realm of the CIA or other intelligence organizations, but actually commercializing it would require the involvement of private business interests. In a way, this issue can be restated by arguing that American business has the opportunity to play the leading role in protecting itself from foreign influence, with the aid of the
intelligence community, but it would be the intelligence community that would be in the position to decide whether or not to carry out economic espionage and what to do with the results of any such activities.

The economic implications of actual or potential government intelligence support of private business have to take into consideration one thing first and foremost. Even competitive intelligence is only one of the components of a full-spectrum information-gathering program. No matter how good your defenses against espionage are, they cannot do more than merely supplement simple market research and business intelligence. Economic counter-intelligence may help a company hold its own against hostile competitors, but it will never be the only thing that wins the battle.

The relevant social (or ethical) considerations are somewhat complicated. Again, from a legal perspective, there is nothing wrong with protecting trade secrets and even enlisting the active help of the government to do so. On the other hand, it is still not entirely clear how receptive the intelligence community is to this new mission, and how vigorously agencies like the CIA and FBI would carry it out. And there is always a risk that a company that is able to secure counter-intelligence assistance from the government will find itself being accused of gaining unfair advantage over others that are not, even if those companies have access to the same kind of support. What kind of effect this could have on company financials is hard to predict without empirical evidence, but it is not too hard to imagine a situation where a company that is perceived to have a cozy relationship with the government finds itself the target of extensive criticism. Major corporations and defense contractors are, of course, used to situations of this
type, but the effect of a grassroots negative publicity campaign on, say, a small software company could be significant.

Finally, the kinds of technological considerations that are present in this discussion have to go back to the proposals for a government-run clearinghouse of economic intelligence. It may be hard to imagine initially, but over the past decade or so, the government has actually done an excellent job of collecting, organizing and presenting open-source information, at least about itself and about America. All sorts of reports, white papers, policy documents and statistics can now be accessed through various government websites and databases, many of which are quite elaborate from an information science point of view. The policy of disseminating foreign economic information may still have to be developed, but the actual technological backbone for a robust dissemination framework is already in place.

Just as this discussion started with a look at the spectrum of information-gathering activities, it should conclude with a similar overview of how and where the government can best use its information-gathering capabilities to help the private world. Least controversial, and probably easiest to implement, would be a concerted effort to collect open-source intelligence on the corporate level; in a sense, to move from something like the CIA World Factbook and the Library of Congress Country Studies to publications that collect present information on the world’s leading companies in particular industries. Here could also fit activities like databases of annual reports or corporate filings, press releases, marketing materials and other grey literature, including potentially both original versions and translations, though not analysis or evaluation. The CIA is already placing a premium on collecting open-source materials; coupled with the
government's experience in designing and maintaining electronic libraries and databases, a service of this type would be invaluable, particularly to smaller and medium companies that do not operate in-house research centers and do not have the luxury of hiring information consultants. Beyond the general ethical argument that the government should not involve itself with expenses to promote a general favorable business environment, this kind of initiative would be hard to argue against. The next step on the scale would involve either general counter-espionage education of corporates or possibly specific advice to companies that are being threatened or have been specifically identified as being vital to the national interest. Increasing enforcement of both U.S. economic espionage law and any applicable international statutes would be next. Finally, actual economic espionage if not on behalf, then certainly for the benefit, of American industry, is hard to imagine, but still not outright impossible. If a particular foreign company possesses a trade secret that gives it an advantage over U.S. competitors, thus threatening U.S. economic security and well-being, much of the current thinking about the relationship between government intelligence and private business does not endorse acquiring that secret and passing it along to American companies to be exploited and commercialized, but nor does it unambiguously rule such a course of events out. Active espionage of this kind would have to be extremely infrequent, though, and certainly would have to be initiated via government policy, not private business request.

Works cited:


Winkler, I. (2005). *Spies among us: How to stop the spies, terrorists, hackers, and criminals you don’t even know you encounter every day*. Indianapolis: Wiley.

