Espionage, Economic and Industrial

Espionage is the stealing of secrets and is conventionally associated with military conflict. But commercial organisations also have secrets and their theft is a form of espionage, industrial espionage. Economic espionage is a less common term and refers to the threat to national security posed by the theft of secrets, which would weaken not the military strength of a country but its economic competitiveness. US export controls to prevent the flow of high technology information to the Soviet Bloc deftly confused economic with military threat in the notion of dual use technology, a notion that nicely included the Japanese within the military threat to the United States.

In its military association, espionage is akin to many other management terms. The idea of rallying the forces of an organisation to beat an external enemy is long established, especially in marketing and strategy. Military metaphor might satisfy the needs of leadership, but it is less appropriate to new forms of organisational structure. The virtual organisation, the network organisation, and a general appreciation that firms co-operate as they compete do not easily accommodate a fundamental model of us versus them. It is questionable whether the notion of espionage should be extended beyond its strict military application. The problem lies in the nature of information. As the economy becomes increasingly information-intensive, it becomes increasingly obvious that information is a valuable resource. Yet, because its characteristics are
very different from those of other goods, information cannot be treated like other valuable resources. The organisation tends to hoard and guard its information, seeing its capacity to innovate and compete as a function of how much information it has and how little its competitors. This is information mercantilism and it is unsustainable. Organisations must give information if they are to acquire information. Organisations which refuse to give, may lose information anyway. It can be taken by assault through takeover, by agreement through merger or joint venture, or it can be taken by stealth. The last may be the easiest to arrange.

Both efforts to steal information and the propensity to feel that the organisation should be an information fortress suggest that precautions should be taken to prevent the loss of information through industrial espionage. As these may be implemented while the organisation is itself striving to acquire information through its own industrial espionage, that disapproval is directed not at the game itself, but at losing. Indeed, so great may be efforts to avoid losing that no one wins. This occurs when the steps taken to discourage industrial espionage are so exhaustive that they prevent, or at least disrupt, other information transactions, and especially those which bring in information from the outside world, information that the organisation requires for its innovation. In the midst of organisational and market failure, these transactions are often effected by other means, by individual employees exchanging information in their own personal networks. As these employees are trading in information on their own account and primarily for their own benefit, and are quite incapable of distinguishing between the organisation’s information and their own, it is hardly surprising that their activities are often confused with espionage. Efforts made to prevent these activities on the grounds of guarding the organisation’s innovation and
thereby maintaining its competitiveness may actually deprive the organisation of the information it requires for the innovation it needs to be competitive.

As the belief that information should be guarded has grown stronger, so has the conviction that steps must be taken to prevent industrial espionage. As espionage becomes more determined, so do deterrents. Modern observers can be taken aback by the often casual attitude towards espionage of the entrepreneurs of the British Industrial Revolution. They appreciated that Continental visitors were often spies and yet still showed whatever there was to see, arguing that their own innovation would be faster than that of any imitator. But they were also practical, appreciating as much as the modern entrepreneurs of Silicon Valley that only a knowledgeable market will buy new technology.

It can be argued that the innovation of the Industrial and Agricultural Revolutions depended on technique rather than science, that innovation is now derived from government policy and corporate strategy rather than artisan endeavour. Innovation is seen as the product of system – political, organisational, managerial. If espionage is a threat to innovation, it is also a threat to system and to interests which prefer to believe that innovation is an output of scientific qualifications, of large organisations, of R&D laboratories, of investment in research, of managed process. Thus, for example, the patent system is preserved and strengthened not so much because it protects and stimulates innovation as because it fits within a system of beliefs about innovation. Eradicating industrial espionage fits equally well.
Attempts to eradicate industrial espionage tend to leave the espionage untroubled and innovation much damaged. Secrecy and need-to-know regimes impede information flow and transactions in personal networks, and would ultimately force organisations to innovate in isolation. Preventing this fate is the conviction of those who actually do innovate that their innovation is dependent on the efforts of others, that this information cannot be acquired unless other information is given in return, and that individuals are best equipped to effect these transactions. These individuals are also well able – as systems of innovation apparently are not – to distinguish between a transaction which exchanges tacit information for other tacit information and one that exchanges extremely explicit information for an envelope stuffed with banknotes. The latter may transfer specific information, but is an inadequate means of technology transfer: the former, together with mobility of human containers of information, is as essential to innovation now as it was 200 years ago. Institutionally, though, even the information exchange of the Mecca of high technology innovation is totally unacceptable.

“ There is no way to know who is listening….. One experienced listener remarked about The Lion and The Compass, a popular Silicon Valley bar: ‘If you really want to spy, just pull up a stool and listen’.” (Bronson, J. G., ”Unfriendly Eyes”, IEEE Transactions on Professional Communication. 30.3 (1987), 173-178.)

Bibliography


