

Industrial espionage: window of opportunity

Peter J. Phillips & Gabriela Pohl

To cite this article: Peter J. Phillips & Gabriela Pohl (2025) Industrial espionage: window of opportunity, Information Security Journal: A Global Perspective, 34:2, 143-155, DOI: [10.1080/19393555.2024.2378755](https://doi.org/10.1080/19393555.2024.2378755)

To link to this article: <https://doi.org/10.1080/19393555.2024.2378755>



© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.



Published online: 14 Jul 2024.



Submit your article to this journal [↗](#)



Article views: 958



View related articles [↗](#)



View Crossmark data [↗](#)

Industrial espionage: window of opportunity

Peter J. Phillips and Gabriela Pohl

Faculty of Business, Education, Law and Arts, University of Southern Queensland, Toowoomba, Australia

ABSTRACT

Technological solutions cannot completely protect companies and governments from human actors driven by money, greed, or simply the thrill of the steal. In fact, each technological countermeasure for industrial espionage is itself the product of human decision-making attempting to preempt and inhibit the decisions and actions of the industrial spy. Nobody knows for sure who the spy is. And the spy doesn't know for sure that he hasn't already been detected or, even if he hasn't, whether his plans will succeed, and his desired payoffs attained. Searching, deciding, detecting, and stopping the industrial spy when both sides of the game face risk and uncertainty is the subject matter of this paper. We focus on closing the spy's window of opportunity.

KEYWORDS

Decision-making; detection; industrial espionage; search; window of opportunity



1. Introduction

People have spent a lot of money trying to protect their secrets, and other people have spent a lot of money trying to steal them. Danielson (2009, p. 503) defines economic espionage as “... the act of targeting or acquiring trade secrets from domestic companies or government entities to knowingly benefit a foreign state.” Following Danielson, Wagner (2012, p. 1040) defines industrial espionage as being “the same as economic espionage, except that rather than benefiting a foreign government, it benefits another private entity.” Lots of decisions are made – by both the firm and the spy – under conditions of risk and uncertainty. A company doesn't know everything about the threat it faces from economic or industrial espionage, and the spy and the spy's handlers don't know if they will get away with it. Despite this, there haven't been any significant attempts to use decision theory or information economics to get the edge on the “insider” industrial spy. We investigate this potential application of decision theory.

Industrial espionage has become something of an umbrella term (Hou & Wang, 2020) encompassing the different types of threats, from within and without, that are directed toward stealing a company's secrets. Traditionally, industrial

espionage involved the physical theft or copying of documents, plans, formulas, prototypes, or equipment. The modern spy might achieve such objectives by breaching the firm's cybersecurity. Obtaining something as physically intangible as a company's proprietary computer code might be the spy's objective. Regardless of the specific form of espionage, whether or physical or cyber, a common element in cases of industrial espionage is the cooperation of insiders. In fact, up to 85% of cases involve insiders (Hou & Wang, 2020, p. 7). This has prompted researchers to study “insider threats,” with much effort devoted to determining the motivations that prompt people to spy or facilitate spying against their own company with the hope that a better understanding of this behavior would permit the design of more effective countermeasures.

An insider has legitimate access to the company's systems and/or physical buildings (e.g., factories, workshops, administration etc.) though, of course, this access will probably have restrictions that the spy might need to circumvent. A standard typology of insider threats encompasses three types of insiders: (1) the self-motivated insider who is not working for anyone but themselves; (2) the recruited insider, who has been hired or somehow coerced or convinced by a third party to spy for

CONTACT Peter J. Phillips  phillips@usq.edu.au  Faculty of Business, Education, Law and Arts, University of Southern Queensland, Toowoomba 4350, Australia

© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

them; and (3) the planted insider, who has been trained by a third party all along with the specific objective of eventually gaining employment at the target firm (Homoliak et al., 2019, p. 9).¹ What motivates these individuals? Whitty (2021, p. 921) lists eight motivations, including a desire to prove one's cleverness. Homoliak et al. (2019, pp. 9–10), based on their review of earlier research, list three common motivations: (1) financial, which may emerge from a desire to earn extra money to fund a better lifestyle or a desire to recover from financial losses or debts, which is something that a recruiter may exploit; (2) political, which may produce a rift between the insider and the firm, leading to collaborations with more “like-minded” entities against the firm; and (3) personal, which may involve a recruiter exploiting an insider's “darkest secrets” (i.e., blackmail). Once in place, these insiders are an unquantifiable risk for the target firm. However, industrial spies face much risk and uncertainty, as do the handlers, especially if the spy's vices, the very vices that make the spy exploitable in the first place, increase the possibility of exposure. In situations where risk and uncertainty engulf the decision-making processes of all parties, keeping a clear mind is not always easy. And the consequences of failing to do so may be felt for a long time afterward.

A classic example of this is reported by Sibley (1999, p. 95) who pointed out that the conventional wisdom in America regarding the nature of the entirety of Soviet interwar espionage was shaped by the attention given to the Hiss-Chambers and Rosenberg spy cases. Alger Hiss held various positions in the US government. In 1948, he was named by Whittaker Chambers (a member of the US Communist Party) as a communist. Furthermore, Chambers claimed that Hiss was involved in espionage, a much more serious charge. Hiss was eventually given a prison sentence for perjury. He served three years. Julius Rosenberg worked for the Army Signal Corps Engineering Laboratories in the 1940s. He was recruited by the Soviet Union (NKVD or Internal Affairs Commissariat) in 1942. During his time as a Soviet spy, he passed on research about electronics, communications,

and radar. He was arrested in 1950 and both he and his wife were executed in 1953.

Both cases created the impression that Soviet espionage was centered on two targets: (1) government departments in Washington D.C.; and (2) atomic research. In fact, Soviet espionage during the interwar period was much more widespread. It targeted things besides atomic research and it did so in places other than Washington D.C. In fact, as Sibley (1999, p. 95) notes, “[Rosenberg] supplied far more information about military electronics than he did about the atomic bomb.” When a decision-maker focuses on a particular risk like “Soviet espionage in Washington and at atomic research facilities” without assessing concurrent risks like “Soviet espionage outside Washington focused on military electronics” it is called narrow framing.

Narrow framing distorts the allocation of resources² and might cause other errors besides, some of which can have long-lasting effects. Sibley (1999, p. 96) argued that the consequences of narrow framing in this case were significant. When evidence of widespread Soviet espionage came to light at the beginning of the Cold War, says Sibley (1999), it was these revelations, not solely the Hiss-Chambers and Rosenberg cases, which led to a severe reaction by the Federal Bureau of Investigation (FBI) and other government agencies. The result was an “increasingly zealous official security apparatus” and “further polarisation of relations between the United States and Soviet Union” (Sibley, 1999, p. 96).

Military electronics or “the bomb” spring to mind as prime targets of spies. But what about agricultural technology? Hvistendahl (2020) relates the story of a plot to steal genetically modified seeds from U.S. companies Monsanto and Dupont Pioneer. Even deep-sea cables are not safe from espionage. Bilton (2019) reports that new American technology installed on telecommunications cables far beneath the ocean was quickly copied, re-created, and enhanced by a Chinese competitor. The target of the theft might not even be physical. It could be lines of code. American Superconductor (AMSC) lost almost \$1 billion after an engineer at the company was enticed by a Chinese competitor to steal code that regulated

the flow of electricity from wind turbines (Sears & Isikoff, 2013). And, of course, while all this has been going on, industrial espionage in more traditional sectors, like aviation engineering, continues (e.g., BBC News, 2018). And it is getting easier (Hooker, 2016). In mid-2022 the Federal Bureau of Investigation (FBI) and MI5 issued a direct warning about Chinese efforts to steal Western technology. Over the next few days, this was a top story across most major news platforms (e.g., Corera, 2022; Lipinski, 2022; Sevastapulo & Rathbone, 2022). The FBI and MI5 chiefs indicated that hacking represents a significant component of this threat. But the old-fashioned kind of secret-stealing still takes place. When the (insider) industrial spy comes to believe that there is a window of opportunity, he begins the decision-making process that may eventually lead to him stealing from his firm. It emerges as a possibility, therefore, that the firm may impose countermeasures designed to disrupt the spy's window of opportunity. Formally, this amounts to an attempt to disturb the very foundation of the spy's decision-making process, the structure of his problem space.

2. The structure of the problem space

If an enemy submarine dives in response to aerial reconnaissance, what is the pilots' optimal course of action? What is the best allocation of resources if you are trying to build a naval blockade to protect an area from enemy submarines? Decision theory emerged alongside operations research and game theory during the middle part of the 20th century and some of the liveliest examples stem from applications developed during World War II (see McCloskey, 1987). The purpose of decision theory (or information economics) is to search for alternatives, identify possible outcomes and their probabilities, and rank the alternatives from best to worst. Naval blockades against submarines seem quite different from decisions about capital allocation in business, or portfolio allocation in finance, or decisions about cybersecurity, or the industrial spy's choices. But there is an underpinning structure, and this is what decision theory hangs its hat on.

The industrial spy works under conditions of risk and uncertainty. The spy's response to risk

and uncertainty is to delineate the problem space. The exact nature of this delineation will usually reflect the spy's background and experience. For example, in thinking about a problem involving the allocation of resources throughout a city (e.g., recreational facilities), the engineer might picture the city as a grid, the social worker as areas of higher or lower income, the teacher as over or underperforming school districts, and the police captain as pockets of high or low crime rates. Likewise, the industrial spy will delineate the problem space differently if he or she is an accountant, engineer, computer programmer, or sales executive.³ We must add to this, of course, matters of ideology, the spy's financial position, his or her tendency to seek revenge, and pursuit of power. This tends to brush up against the spy's motives, but it is important to keep in mind that a spy who seeks financial payoffs may frame his problem and delineate the problem space distinctly from one who seeks to acquire and disseminate some technology or other for humanitarian ends. The outcomes and the odds that are attached to them are distinct in each case.

The industrial spy identifies some set of characteristics that define the boundaries of a "search" (see Stigler, 1961) relating to the payoffs that he or she desires, whether financial, patriotic, or humanitarian. Information gathering cannot go on forever and people naturally look for ways to limit the search process. For example, an investor might only be interested in companies with dividend yields above 6% or a consumer might only be interested in exploring the options that are available at the three stores closest to where she lives. Figure 1 presents a sketch of a situation where the decision-maker initiates a search within a delineated problem space represented by closed or bordered boxes. Through search, the decision-maker gathers information (y) used to uncover alternatives (i) and their possible outcomes (x).

This process is performed in the window of opportunity. By performing it, the industrial spy builds a blueprint of the problem space within which the available actions, if he or she chooses to go ahead with them, are expected to play out. This is not static, but dynamic. Adjustments will take place along the way. Information continues to flow. Mostly, decision-makers are reluctant to overturn

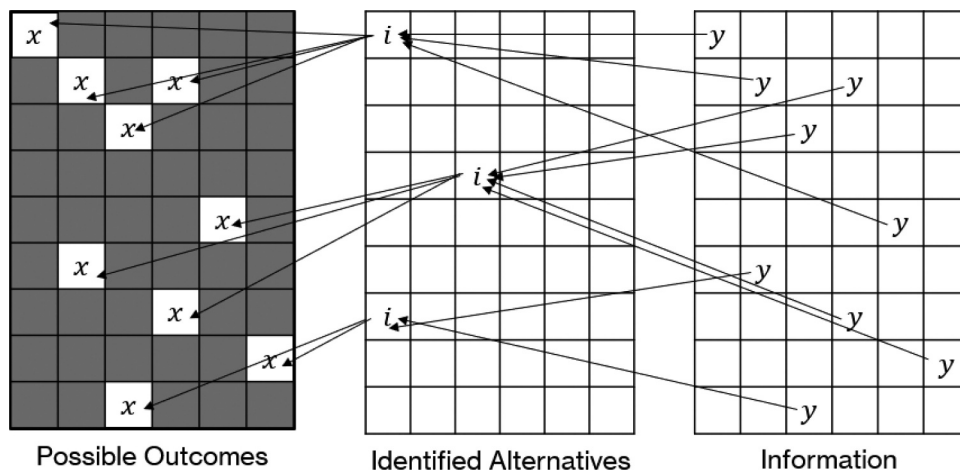


Figure 1. Information, alternatives, outcomes.

what they have invested time and effort in creating (i.e., sunk cost fallacies). And they come to value what they have more than what they don't have (i.e., endowment effect). Once the decision to act has been made, there is usually no going back. The spy makes his or her selection by ordering the alternatives that have been uncovered by the search. The ordering might be perfectly rational, in which case it would be one that maximizes von Neumann and Morgenstern's (1947) expected utility. Or it might be shaped by various psychological factors, in which case it would be better modeled by Kahneman and Tversky's (1979) prospect theory.

The latter opens the path for more interesting accounts of the spy's decision-making process, and importantly, opens the door to designing ways to disrupt it. That is not to say that the expected utility maximizer does not make mistakes. Such decision-makers can and do make mistakes. But those mistakes are not systematic, and he or she will not be distracted by side issues. All that matters to such a rational decision-maker is the alternatives, outcomes, and probabilities which he or she sees clearly. On the other hand, the decision-maker portrayed by Kahneman & Tversky, and who appears in various guises throughout behavioral economics, errs systematically.

For instance, when the industrial spy looks for and, later, evaluates alternatives, he or she may have a reference point in mind. The reference point is the central concept of prospect theory. A reference point is an outcome, x , that holds

a special place in the decision-maker's process. The reference point might be a payoff of zero or the maintenance of the status quo, it might be an idol or rival's achievements, or it might be a goal or aspiration (Lopes, 1987; Lopes & Oden, 1999). Whatever it is and whatever its origin, the reference point is the outcome against which other outcomes are framed as gains or losses. Looking for and valuing outcomes relatively rather than absolutely can lead to errors.⁴ A positive payoff (e.g., \$1,000,000) might be framed as a loss if the reference point is \$2,000,000. More than this, the reference point is the point at which risk preferences switch back and forth between risk seeking and risk aversion.

Above the reference point, after gains have accrued or in expectation of them, the decision-maker is risk averse. Below the reference point, after losses have been incurred or in expectation of them, the decision-maker is risk seeking. While the gains and losses might refer to the act of industrial espionage (e.g., money made by selling information or a key opportunity closed, such as a new security measure put in place at the organization), the industrial spy's reference point might be exogenous to industrial espionage. The spy might have experienced gambling losses and tries to recoup them through selling the firm's information, or the spy might have been passed over for a promotion or a desirable posting. Once underway, the gains and losses stemming from the espionage activities dynamically shape the valuation of

outcomes. Thwarted on previous attempts to steal information, the spy might become risk seeking, looking for that last ace in the deck.

The industrial spy whose decisions are described by prospect theory also has a distorted perception of the probabilities, p 's. Specifically, such decision-makers overweight the chances of experiencing an unlikely outcome and underweight the chances of experiencing a likely outcome. This is driven by the spy's hopes and fears. If bad outcomes are *least likely* (i.e., probabilities closer to zero), overweighting of those low probabilities reflects the fear that something bad will happen while the attention focused on zero reflects the hope that that it won't. At the other end of the distribution, where good outcomes are *most likely*, underweighting of high probabilities signals the fear that a good outcome won't occur while the attention focused on certainty (i.e., probability = 1) reflects the hope that it will.⁵ The psychological factors that produce these tendencies are wedges which open cracks in the spy's problem space.

3. The spy's window of opportunity

While a company can be hacked or infiltrated from the "outside," many industrial spies are insiders or work with an insider's help:

In 1994, the FBI reported that its economic counter-intelligence unit had information that nearly 50% of research and development firms had a trade secret theft, and 57% reported repeat of multiple thefts. An employee most often accomplished the thefts.⁶

And a specific example:

Harold C. Worden was a 30-year employee of the Eastman Kodak Corporation who established his own consulting firm upon retiring from Kodak. During his last five years at Kodak, Worden was project manager for what was known as the 401 machine. This is a new machine designed to inexpensively produce the clear plastic base used in consumer film. The base is lined with emulsions using a secret formula that determines the quality of the photographs. When Worden retired, he took with him thousands of documents marked "confidential" about the development the 401 machine, and he recruited his successor to continue providing confidential information. A Kodak spokesman said the numerous drawings, plans, manuals and other documents removed by Worden were worth millions of dollars to the company, even though Worden by the time of his arrest had received only \$26,700 for selling

the information. The market share at risk as a result of Worden's activities could have been in the billions of dollars.⁷

The methods are now more technologically sophisticated, but the objective remains the same. In 2024, the U.S. Department of Justice (United States Department of Justice DOJ, 2024) announced the indictment of seven Chinese nationals for conspiracy to commit computer intrusions. The indictment details a 14-year-long conspiracy to target "... journalists, political officials, and companies to repress critics of the Chinese regime, compromise government institutions, and steal trade secrets." This came a year after other indictments were handed down against an employee of General Electric, Zheng Xiaoqing. According to the BBC (Yong, 2023):

... the US citizen hid confidential files stolen from his employers in the binary code of a digital photograph of a sunset, which Mr Zheng then mailed to himself. It was a technique called steganography, a means of hiding a data file within the code of another data file. Mr Zheng utilised it on multiple occasions to take sensitive files from GE [General Electric]. The information Zheng stole was related to the design and manufacture of gas and steam turbines, including turbine blades and turbine seals. Considered to be worth millions, it was sent to his accomplice in China. It would ultimately benefit the Chinese government, as well as China-based companies and universities.

The company can manipulate the reality and perception of the (inside) industrial spy's window of opportunity. Any window of opportunity, though it might only be a few days or even a few moments, is a habitat for a problem space in which the industrial spy can construct the blueprint for his or her plans and schemes. It follows that the company might benefit from paying attention to the industrial spy's window of opportunity and the possibility of disrupting the problem space that the spy is building within that window of opportunity once the spy notices that he or she has one. We explain the basic outlines of a plan to disrupt the industrial spy by upsetting his decision-making process.

3.1. Alertness

The industrial spy's opportunity is a monetary opportunity or "monetary equivalent" if there are

non-monetary motives. While the firm might not always be able to ensure that every door is locked, so to speak, steps can be taken to reduce the spy's alertness to opportunity presented by an open door. Being alert does not mean that the spy is actively searching for opportunities. The spy is not trying every doorhandle, but the spy *notices* when he or she comes across an unlocked door. The firm must try to keep all the doors locked *and* reduce the chances that the alert spy will notice an unlocked door. But what is the spy alert to?

The best answer comes from that intersection of decision theory, search theory, and the (elusive) theory of entrepreneurial discovery (e.g., Kirzner, 1973, 1979, 1982, 1985, 1992a, 1992b). Simply put, the industrial spy is alert to an "arbitrage opportunity." The difference in value of the information to him or her *within* the firm vis-à-vis *outside* the firm. He or she must feel capable of bridging that divide by stealing information and successfully exporting it out of the firm. The question, then, is how to direct this type of alertness to the benefit rather than the detriment of the firm.

To redirect it, we would have to know its source. And this is not easy to identify. Gaglio and Katz (2001, p. 95) explain:

To date, investigators have examined issues such as whether entrepreneurial opportunities are the result of serendipity or deliberate search (Koller, 1988; Peterson, 1988). Numerous search behaviours have been profiled including the source of the idea (W. Long & Graham, 1988; Peterson, 1988); search strategies; and amount of search effort (Busenitz, 1996; Gilad et al., 1988; Kaish & Gilad, 1991). In addition, the influence of the entrepreneur's social network on search strategies and boundaries have been explored (Aldrich & Zimmer, 1986; N. Long, 1979; Pekerti, 1985). Evaluation strategies (Crawford, 1980; W. Long & McMullan, 1984) have been studied. Finally, some have tried to map the stages or phases of the opportunity identification process (Herron & Sapienza, 1992; W. Long & McMullan, 1984) and document the length of time needed in this process to shape successful business opportunities. (Singh et al., 1999; Van de Ven, 1980)

In the end, nothing has been identified as *the* key to entrepreneurial alertness. Entrepreneurs just seem to be better at spotting opportunities, realizing the potential of those opportunities, and acting on that realization. Nobody knows why exactly. But some

interesting ideas have emerged that could be used to redirect the alertness of the industrial spy. These come from the intersection of decision theory, orthodox and behavioral, with the concepts of search, discovery, and alertness.

Valliere (2013), for example, argues that everyone uses schemata (mental frameworks) to make sense of the world. These include the narratives, analogies, and experiences that we mentioned earlier with reference to problem space delineation. Alert people, including entrepreneurs, use different schemata to ordinary people. But alertness is not set at birth. It can be "inculcated and enhanced" (Valliere, 2013, p. 430). We would argue, therefore, it can be redirected. As Valliere (2013, p. 438) explains, it is possible to teach entrepreneurial alertness by exposing people to analogies to foster the development of new schemata and the application of the new schemata to relevant situations. We venture to suggest that formal entrepreneurial education within firms may redirect the alertness of the industrial spy along more favorable channels while benefiting the rest of the workforce (and the organization) in the bargain. Essentially, overwriting potentially nefarious schemata with positive ones or, if one prefers, imprinting positive schemata that are more difficult to overwrite with nefarious ones. It is just one of many possible suggestions that can be derived from the research on alertness.

3.2. Alternatives

If there is a spy who has been alert enough to spot a window of opportunity, the spy must delineate and fill in the problem space with alternatives, outcomes, and probabilities before selecting the best course of action. This might take some time. Also, the spy might not yet have a ready buyer for the information he or she has now realized can be stolen.

The flow of information is central to the spy's ability to uncover alternatives and their possible outcomes. It is also central to the spy's determination of the (subjective) probabilities that are attached to those outcomes. The first line of defense for the firm, therefore, is to impede the spy's flow of information. Notice, however, that this is different from hiding the information that

the industrial spy might steal. That is a separate matter and we have assumed that the spy has, in fact, already spotted an opportunity. He or she is at least aware of the existence of information that has a value if it can be obtained and exported outside the firm. What the firm seeks to impede here is information that enables the spy to delineate and fill in the problem space, either completely or to the spy's satisfaction. This is information about the alternatives he or she has with regards to stealing the information he or she knows to exist (e.g., where the information is stored, where the documents are kept, whether it is feasible to steal a key to a room or steal another person's passcode, whether the information can be printed or copied and smuggled out of the firm physically etc.).

"Information dams" can be established around all the details that would be necessary for an industrial spy to know before feeling comfortable enough to rank the alternatives and make a choice. For example, where the information is kept and who has access to it. Those with access to the information, which might include the spy, might be prevented from knowing the details of the way in which the information has been secured, physically or electronically. Information dams prevent a clear alternative from presenting itself and, if it does, make it more difficult to determine the outcomes that might be experienced by choosing it. The objective is to prevent an ordering of the alternatives in the first instance and, second, prevent an optimal ordering of those alternatives should they be uncovered.

3.3. Outcomes

Now assume, as we must, that the dams might be breached. The spy uncovers at least one way of achieving the objective (i.e., capitalizing on the arbitrage opportunity). The firm's information defenses that concern us now are those that distort the spy's outcomes, x 's. The outcomes that most people probably have in mind are monetary payoffs or the intangible things that one might associate with espionage, such as feelings of power or the thrill of being the main character in one's own secret game. As the spy searches for possible outcomes that might be experienced if one of the

available alternatives are chosen, he or she relies on the routines established within the firm.

The importance of routines within firms has been noted by management scientists, decision theorists, and economists. Some researchers have said that "routines are genes" (Nelson & Winter, 2002, p. 30). Given this, Nelson and Winter (1982, p. 134) suggest, "As a first approximation, therefore, firms may be expected to behave in the future according to the routines they have employed in the past." These routines are like a tether that the industrial spy can fasten himself to as he navigates his problem space. By introducing subtle randomness into the routines that pertain to the management of sensitive information, the firm can disrupt the industrial spy. If the how, when, and where of sensitive information is clear to the industrial spy, he or she feels that he or she is on sure footing. And vice versa.

As a specific example, consider that the industrial spy, along with everything else, is looking for the excuses that can be used if he or she is detected. If, for instance, the spy knows that he or she must access a building that he or she normally should not be in, how will he or she explain his or her presence? An excuse is a type of contingent alternative with its own outcomes. That is, it is an alternative (one among many perhaps) that will be enacted contingent on being detected while following through with his primary alternative (i.e., the method he has chosen to steal the information). The more structure that the industrial spy can wrap around the entirety of the available alternatives, contingent alternatives, and outcomes the less uneasy the spy feels. The routines that exist within every firm provide an important part of this structure. Introducing subtle randomness, such as the changing of passcodes or passkeys out of schedule, disrupts the spy's process.

3.4. Probabilities

Of all the things that the firm might target, the most promising is the odds that the spy attaches to the outcomes. The things that we have just mentioned – information dams and subtle randomness to routines – upset the spy's ability to

gauge the odds. In addition, the firm can target the “odds of detection.” According to classical economic analysis of crime (i.e., Becker, 1968), the risk seeking offender is much more sensitive to changes in the odds of detection and punishment than he or she is to changes in severity of the punishment while the risk averse offender is more sensitive to changes in the severity of punishment. Becker (1968, p. 177) offers a simple model of criminal behavior:

$$O_j = O_j(p_j, f_j, u_j)$$

Where O_j is the number of offenses the criminal commits, p_j is the probability of conviction per offense, f_j is the punishment per offense, and u_j is a catchall for all other factors. The offender’s expected utility from committing an offense is:

$$EU_j = p_j U_j(Y_j - f_j) + (1 - p_j) U_j(Y_j)$$

Where Y_j is the offender’s income, monetary plus psychic, from an offense. U_j is the utility function and f_j is the monetary equivalent of the punishment. The partial derivatives with respect to the probability of conviction and the severity of the punishment respectively are:

$$\frac{\partial EU_j}{\partial p_j} = U_j(Y_j - f_j) - U_j(Y_j) < 0$$

$$\frac{\partial EU_j}{\partial f_j} = -p_j U'_j(Y_j - f_j) < 0$$

The firm cannot do much about the severity of the punishment as far as the legal penalties are concerned (e.g., jail) but they can shape the punishments that are dispensed within the organization (e.g., dismissal or automatic referral to the Federal Bureau of Investigation *etc.*). Furthermore, the firm can certainly influence the odds of detection. In doing so, however, the things that we have learned from behavioral economics since Becker (1968) are relevant to the effectiveness of any such measures that the firm might take.

In Becker’s analysis, the offender is either risk seeking or risk averse. The offender does not oscillate between one and the other. The risk seeking offender is more sensitive to p_j and the risk averse offender is more sensitive to f_j . If this can be assumed to apply generally, it follows that the

offender whose decisions are described by prospect theory will be more sensitive to changes in the likelihood of detection when he or she is in the domain of losses (and therefore risk seeking) and more sensitive to changes in the severity of punishment when he or she is in the domain of gains (and therefore risk averse). And the offender will oscillate between being more sensitive to changes in the odds of detection and changes in the severity of the punishment. The deterrence of the industrial spy requires attention to both the odds of detection and the severity of the punishment.

Probability weighting works both for and against the firm as it tries to influence the industrial spy’s estimate of the odds of success. As the firm pushes the probability of detection higher, the spy’s tendency (if he is described by prospect theory)⁸ to underweight the odds makes the spy less sensitive, across moderately high probabilities, to the increased odds of detection. This changes as the probabilities continue to increase and approach one. Here the spy becomes much more sensitive to an equivalent change in the odds. Across the moderately high range, he or she does not increase the odds of detection in his or her own mind by as much as he or she should (by as much as the expected utility maximizing decision-maker does). On the plus side, this undermines the spy’s judgment, potentially leading the spy into error. On the downside, he or she is more likely to act than one might expect given the steps that the company has taken to increase the odds of detection.

4. Anchoring the firm’s expected losses

In choosing among countermeasures designed to reduce the risk of industrial espionage, the firm’s decision-makers are guided by the costs expected to be incurred should the firm fall prey to the industrial spy. Estimating these costs and factoring them into the firm’s decision-making process is not an easy task. The evaluation of potential losses to industrial espionage is made more difficult by the publicity accorded to some cases. The financial losses revealed in these high-profile cases may become “anchors” for decision-makers in other firms. When asked to make a numerical prediction people think of an initial number and then make an

adjustment from that anchor.⁹ The adjustment is usually insufficient. While the anchor may derive from the way the problem is presented or from some preliminary thinking about potential gains and losses, one of the more stunning discoveries that psychologists have made is that an anchor can be irrelevant to the problem itself. Tversky and Kahneman (1974, p. 1128) explain how an arbitrary anchor was created by the spinning of a “wheel of fortune:”

In a demonstration of the anchoring effect, subjects were asked to estimate various quantities, stated in percentages (for example, the percentage of African countries in the United Nations). For each quantity, a number between 0 and 100 was determined by spinning a wheel of fortune in the subjects’ presence. The subjects were instructed to indicate first whether that number was higher or lower than the value of the quantity, and then to estimate the value of the quantity by moving upward or downward from the given number. Different groups were given different numbers for each quantity, and these arbitrary numbers had a marked effect on estimates. For example, the median estimates of the percentage of African countries in the United Nations were 25 and 45 for groups that received 10 and 65, respectively, as starting points. Payoffs for accuracy did not reduce the anchoring effect.

The losses from individual industrial espionage cases are not usually reported. We are left with high-profile cases and aggregate estimates of total losses. The veracity of the estimated costs that are reported is open to question. For example, the Washington Post reported in 2014 that an estimate from the Centre for Strategic and International Studies placed the annual cost of cybercrime and industrial espionage at \$445 billion (Nakashima & Peterson, 2014). Other estimates, excluding cybercrime, are much lower. Munsey (2013) put the annual cost of industrial espionage to the US economy at “just” \$13 billion.

When decision-makers are presented with such wide-ranging figures, the potential for error in assessing a given company’s potential losses is enhanced. This is exacerbated by the possibility that any one of these estimates may become an anchor. Furthermore, anchoring interacts with other aspects of decision-making, including reference points and framing. MacDonald (1996)

argued, for example, that industrial espionage has failed to attract academic interest because industrial espionage is ineffective at transferring technology and, therefore, unconnected with innovation, a topic that MacDonald (1996) suggests is of “consuming interest” to academics. Likewise, Zatlin (2008, p. 48) argued:

Worse still, the efforts of economic spies such as Ronneberger¹⁰ were largely wasted because East German industry was unable to make use of the technology they managed to smuggle into the GDR. As one historian has concluded, MfS [Ministry for State Security] agents and officers were aware that narrowing the scientific and technological gap with the West was an “illusionary goal.”

Doubt has since been cast on this conclusion. In the first major study of its kind, Glitz and Meyersson (2020) analyzed the effectiveness of industrial espionage as a tool that a government can use to increase its total factor productivity. Drawing on 189,725 pieces of information received by the East German Ministry for State Security (the Stasi) for the period 1970 to 1989, Glitz and Meyersson (2020) concluded that industrial espionage involving flows of technical information and knowhow from West Germany to East Germany allowed the East German government to significantly increase total factor productivity. In fact, due to its program of industrial espionage, East German total factor productivity was 13.3% higher at the end of the Cold War than it would have been in the absence of industrial spying.

5. Concluding remarks & practical implications

Decision theory or information economics complements efforts to understand the nature and motivation of insider threats, whether more “traditional” in nature or related to cybersecurity. Our focus on working through some of the logic of decision in the context of industrial espionage may be summarized by the following set of problem space delineations and their associated practical implications:

- A window of opportunity, though it might only be open for a few days or even a few

moments, is a habitat for a problem space in which the industrial spy can construct the blueprint for his or her plans and schemes. It follows that the firm should try to disrupt the problem space that the spy is building within his or her window of opportunity.

- The construction of a problem space, with the objective of identifying and ranking actions that can be implemented to achieve an objective (i.e., theft of secrets), can only proceed once an opportunity has been spotted.
- The industrial spy is alert to an arbitrage opportunity, a difference in the value of information within the firm versus its value to outsiders. This “entrepreneurial alertness” may be redirected by the firm into more productive channels. This can be done by giving employees training designed to hone entrepreneurial alertness in contexts and cases that are likely to generate positive rather than nefarious outcomes for the firm. Such positive arbitrage opportunities might pertain to new markets, new products, innovations in production methods, cost savings etc.
- Impeding the flow of information disrupts the spy’s ability to complete the problem space within the window of opportunity. This is distinct from hiding or securing the information that the spy seeks to steal. One way to accomplish this disruption is to establish “information dams” or “diversions” which obscure the nature and location of sensitive information along with other relevant factors such as the nature of the security measures that have been implemented. Information dams make it harder for the spy to identify possible courses of action.
- If the industrial spy has spotted an opportunity and has begun to fill in his or her problem space with the goal of finding the best course of action, and if the information dams have been breached, the firm still has another line of defense. This is the distortion of the possible outcomes of the spy’s alternative courses of action. The search for outcomes that may be the consequence of a particular choice can be made easier or harder for the spy depending on the regularity of the firm’s routines.

Routines can make the spy feel more sure-footed. Introducing subtle randomness disrupts the spy’s decision-making process.

- Finally, the firm can attempt to disrupt the spy’s probabilities. Even if the spy has identified a set of possible actions and their consequences/outcomes, there remains the task of figuring out the likelihood of success. Probability weighting can work for and against the firm’s countermeasures. While the firm might increase the odds that the spy will be detected, the spy may, at the same time, underweight those odds. The countermeasure’s effectiveness as a deterrence is watered down. On the plus side, while the spy might not be deterred, the underweighting of the odds may be pivotal in the spy’s downfall.

We close by highlighting one thing that is not usually mentioned by researchers. This is the importance of the spy’s choice of excuse. In hindsight, the industrial spy’s actions prior to taking the fateful step to steal and disseminate information will make sense. What was the person doing in that facility after hours? Why did he or she use a colleague’s pass card or login? Why did the employee insist on being on certain project teams or on certain shifts? Now we know. At some point, the spy might have been challenged. A security guard might have questioned his or her presence in a part of the building. A colleague might have asked about the use of the colleague’s workstation or accessing the colleague’s desk drawers. At these points, which probably occur in most cases of industrial espionage, the industrial spy makes a choice that is not usually analyzed but which is as important as any of the spy’s other choices. That is, he or she chooses an *excuse*. Like all the choices that the spy makes, the choice of excuse is subject to risk and uncertainty. The risk that the spy bears or the uncertainty that the spy faces when formulating a set of excuses, either beforehand or on the spot, can be increased. Routines are genes, as Nelson and Winter (2002) said. Among other things, they store and carry information. The industrial spy can be disrupted by subtle, unpredictable changes to routines. And the spy can be frustrated by adherence to them. If it boils down to a struggle between who is more alert, the spy or the firm’s managers, this struggle may turn on

who draws more cleverly than the other on the nature of organizational routines as the carriers of information.

Notes

1. Also see Yuan and Wu (2021, p. 3).
2. For a discussion of narrow framing and examples of applications to financial decision-making see Benartzi and Thaler (1995) and Barberis et al. (2006).
3. The roots of this, which are beyond our scope here, run deep into people's reliance on metaphor and analogy (see Gibbs, 1992; Hesse, 1966; Indurkha, 1992; Kittay, 1987; Kuhn, 1979; Lakoff & Johnson, 1980; Prandi & Rossi, 2022) and narrative (see Bouizegarene et al., 2020) to frame their world and the problems they face, including the development of hypotheses about the natural world.
4. The expected utility maximizer evaluates payoffs in absolute terms.
5. This is inverted if good outcomes are least likely. Lopes (1987) and Lopes and Oden (1999) talk of fear and hope. The explanation that we have provided is an interpretation of their explanation for probability weighting.
6. Fischer et al. (2018, p. 501).
7. Western Region Security Office (2001).
8. See Gonzalez and Wu (1999).
9. The anchor is usually numerical, but it needn't be. The idea that East Germany was incapable of transforming stolen technological knowhow into scientific and economic reality is also an anchor and one that prevails until research comprehensive enough to change the narrative emerges.
10. Gerhardt Ronneberger was one of East Germany's most prolific smugglers of industrial secrets from West to East.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

- Aldrich, H. E., & Zimmer, C. (1986). Entrepreneurship through social networks. In D. L. Sexton & R. W. Smilor (Eds.), *The art and science of entrepreneurship*. (Ballinger Publishing) (pp. 3–23). Cited by Gaglio & Katz (2001).
- Barberis, N., Huang, M., & Thaler, R. H. (2006). Individual preferences, monetary gambles, and stock market participation: A case for narrow framing. *The American Economic Review*, 96(4), 1069–1090. <https://doi.org/10.1257/aer.96.4.1069>
- BBC News. (2018, October 11). Chinese man charged with US aviation espionage.
- Becker, G. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, 76(2), 169–217. <https://doi.org/10.1086/259394>
- Benartzi, S., & Thaler, R. H. (1995). Myopic loss aversion and the equity premium puzzle. *Quarterly Journal of Economics*, 110(1), 73–92. <https://doi.org/10.2307/2118511>
- Bilton, N. (2019, June 4). Deep-sea divers and industrial espionage: On the front lines of the new cold war. *Vanity Fair*.
- Bouizegarene, N., Ramstead, M. J. D., Constant, A., Friston, K. J., & Kirmayer, L. J. (2020, July 9). Narrative as active inference: An integrative account of the functions of narratives. Preprint, PsyArXiv.
- Busenitz, L. W. (1996). Research on entrepreneurial alertness. *Journal of Small Business Management*, 34 (4) , 35–44. <https://www.proquest.com/scholarly-journals/research-on-entrepreneurial-alertness/docview/221001969/se-2>. Cited by Gaglio & Katz (2001).
- Corera, G. (2022, July, 8). *China: MI5 and FBI heads warn of 'immense' threat*. BBC.
- Crawford, C. M. (1980). The idea evaluation function in entrepreneurial alertness 109 smaller firms. *Journal of Small Business Management*, 18 (2), 31–40. <https://www.proquest.com/scholarly-journals/idea-evaluation-function-smaller-firms/docview/210773756/se-2>. Cited by Gaglio & Katz (2001).
- Danielson, M. E. A. (2009). Economic espionage: Framework for workable solution. *Minnesota Journal of Law, Science & Technology*, 10 (2), 503–548.
- Fischer, R., Haliobozek, E., & Walters, D. (2018). *Introduction to security* (10th ed.). Butterworth-Heinemann.
- Gaglio, C. M., & Katz, J. A. (2001). The psychological basis of opportunity identification: Entrepreneurial awareness. *Small Business Economics*, 16(2), 95–111. <https://doi.org/10.1023/A:1011132102464>
- Gibbs, R. W., Jr. (1992). Categorization and metaphor understanding. *Psychological Review*, 99(3), 572–577. <https://doi.org/10.1037/0033-295X.99.3.572>
- Gilad, B., Kaish, S., & Ronen, J. (1988). The entrepreneurial way with information. In S. Maital (Ed.), *Applied behavioural economics* (Vol. 2) New York, New York: New York University Press, (pp. 481–503), Cited by Gaglio & Katz (2001).
- Glitz, A., & Meyersson, E. (2020). Industrial espionage and productivity. *The American Economic Review*, 110(4), 1055–1103. <https://doi.org/10.1257/aer.20171732>
- Gonzalez, R., & Wu, G. (1999). On the shape of the probability weighting function. *Cognitive Psychology*, 38(1), 129–166. <https://doi.org/10.1006/cogp.1998.0710>
- Herron, L., & Sapienza, H. (1992). The entrepreneur and the initiation of new venture launch activities. *Entrepreneurship Theory and Practice*, 17(1), 49–55. <https://doi.org/10.1177/104225879201700106>. Cited by Gaglio & Katz (2001).

- Hesse, M. (1966). *Models and analogies in science*. University of Notre Dame Press, Notre Dame.
- Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modelling and countermeasures. *ACM computing surveys*, 52, paper no. 30.
- Hooker, L. (2016, August 23). Are hi-tech spies stealing all your firm's secrets? BBC News.
- Hou, T., & Wang, V. (2020). Industrial Espionage: A Systematic Literature Review. *Computers & security*, 98, paper no. 102019.
- Hvistendahl, M. (2020, August 19). The FBI's decades long fight against industrial espionage hasn't really worked. MIT Technology Review.
- Indurkha, B. (1992). *Metaphor and cognition*. Kluwer Academic Publishers.
- Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2), 263–292. <https://doi.org/10.2307/1914185>
- Kaish, S., & Gilad, B. (1991). Characteristics of opportunities search of entrepreneurs versus executives: Sources, interests, general alertness. *Journal of Business Venturing*, 6(1), 45–61. [https://doi.org/10.1016/0883-9026\(91\)90005-X](https://doi.org/10.1016/0883-9026(91)90005-X). Cited by Gaglio & Katz (2001).
- Kirzner, I. M. (1973). *Competition and entrepreneurship*. University of Chicago Press.
- Kirzner, I. M. (1979). *Perception, opportunity, and profit*. University of Chicago Press.
- Kirzner, I. M. (1982). Competition, regulation, and the market process: An "Austrian" perspective. *Cato policy analysis*. Cato Institute, 18.
- Kirzner, I. M. (1985). *Discovery and the capitalist process*. University of Chicago Press.
- Kirzner, I. M. (1992a). Entrepreneurship, uncertainty, and Austrian economics. In B. J. Caldwell & S. Boehm (Eds.), *Austrian economics: Tensions and new directions* (pp. 68–102). Kluwer Academic Publishers.
- Kirzner, I. M. (1992b). *The meaning of market process: Essays in the development of modern Austrian economics*. Routledge.
- Kittay, E. (1987). *Metaphor: Its cognitive force and linguistic structure*. Clarendon Press.
- Koller, R. H. (1988). On the source of entrepreneurial ideas. In B. A. Kirchoff, W. Long, W. McMullan, K. H. Vesper, & W. E. Wetzel (Eds.), *Frontiers of entrepreneurship research* (pp. 194–207). Babson College.
- Kuhn, T. S. (1979). Metaphor in science. In O. Andrew (Ed.), *Metaphor and thought*. Cambridge, UK: Cambridge University Press, (pp. 533–542).
- Lakoff, G., & Johnson, M. (1980). *Metaphors we live by*. Chicago University Press.
- Lipinski, D. (2022, July 6). Heads of FBI, MI5 issue joint warning on Chinese spying. Wall Street Journal.
- Long, N. (1979). Multiple enterprise in the central highlands of peru. In S. M. Greenfield, A. Strickon, & R. T. Aubey (Eds.), *Entrepreneurs in cultural context* (pp. 123–158). University of New Mexico Press.
- Long, W., & Graham, J. B. (1988). Opportunity identification process: Revisited. In G. E. Hills, R. W. Laforge, & B. J. Parker (Eds.), *Research and the marketing/entrepreneurship interface*. Office of Entrepreneurial Studies, University of Illinois, pp. 209–220. Cited by Gaglio & Katz (2001).
- Long, W., & McMullan, W. E. (1984). Mapping the new venture opportunity identification process. In J. A. Hornaday, F. A. Tardley, J. A. Timmons, & K. H. Vesper (Eds.), *Frontiers of entrepreneurship research* (Wellesley, MA: Babson College) (pp. 567–591). Cited by Gaglio & Katz (2001).
- Lopes, L. L. (1987). Between hope and fear: The psychology of risk. *Advances in Experimental Social Psychology*, 20, pp. 255–295. [https://doi.org/10.1016/S0065-2601\(08\)60416-5](https://doi.org/10.1016/S0065-2601(08)60416-5).
- Lopes, L. L., & Oden, G. C. (1999). The role of aspiration level in risk choice: A comparison of cumulative prospect theory and SP/A theory. *Journal of Mathematical Psychology*, 43 (2), 286–313. <https://doi.org/10.1006/jmps.1999.1259>
- MacDonald, S. (1996). Industrial espionage and innovation. *Interdisciplinary Science Reviews*, 21(3), 209–214. <https://doi.org/10.1179/isr.1996.21.3.209>
- McCloskey, J. F. (1987). U.S. Operations research during world war II. *Operations Research*, 35(6), 910–925. <https://doi.org/10.1287/opre.35.6.910>
- Munsey, C. (2013, November 6). Economic espionage: Competing for trade by stealing industrial secrets. Law Enforcement Bulletin.
- Nakashima, E., & Peterson, A. (2014, June 9). *Report: Cybercrime and espionage costs \$445 billion annually*. The Washington Post.
- Nelson, R. R., & Winter, S. G. (1982). *An evolutionary theory of economic change*. Harvard University Press.
- Nelson, R. R., & Winter, S. G. (2002). Evolutionary theorising in economics. *Journal of Economic Perspectives*, 16(2), 23–46. <https://doi.org/10.1257/0895330027247>
- Pekerti, A. (1985). *The personal networks of successful entrepreneurs* [Ph.D. Thesis]. University of Southern California.
- Peterson, R. T. (1988). An analysis of new product ideas in small business. *Journal of Small Business Management*, 26 (2), 25–31 <https://www.proquest.com/scholarly-journals/analysis-new-product-ideas-small-business/docview/220992896/se-2>. Cited by Gaglio & Katz (2001).
- Prandi, M., & Rossi, M. (Eds.). (2022). *Researching metaphors: Towards a comprehensive account*. Routledge.
- Sears, C., & Isikoff, M. (2013, August 7). Chinese firm paid insider 'to kill my company,' American CEO says. NBC News.

- Sevastapulo, D., & Rathbone, J. P. (2022, July 7). US and UK intelligence chiefs call for vigilance on China's industrial spies. *Financial Times*.
- Sibley, K. A. (1999). Soviet industrial espionage against American military technology and the US response, 1930–1945. *Intelligence and National Security*, 14(2), 94–123. <https://doi.org/10.1080/02684529908432541>
- Singh, R. P., Hills, G. E., & Lumpkin, G. T. (1999). New venture ideas and entrepreneurial opportunities: Understanding the process of opportunity recognition. *Proceedings, 1999 United States Association for Small Business and Entrepreneurship* San Diego, California (pp. 657–671). Cited by Gaglio & Katz (2001).
- Stigler, G. (1961). The economics of information. *Journal of Political Economy*, 69(3), 213–225. <https://doi.org/10.1086/258464>
- Tversky, A., & Kahneman, D. (1974). Judgement under uncertainty: Heuristics and biases. *Science*, 185(4157), 1124–1131. <https://doi.org/10.1126/science.185.4157.1124>
- U.S. Department of Justice (DOJ). (2024, March 25). Seven hackers associated with Chinese government charged with computer intrusions targeting perceived critics of China and U.S. Businesses and politicians. *Press release*.
- Valliere, D. (2013). Towards a schematic theory of entrepreneurial alertness. *Journal of Business Venturing*, 28(3), 430–442. <https://doi.org/10.1016/j.jbusvent.2011.08.004>
- Van de Ven, A. H. (1980). Early planning, implementation, and performance of new organizations. In J. R. Kimberly & R. H. Miles (Eds.), *The organisational life cycle*. Jossey Bass, pp. 83–133. Cited by Gaglio & Katz (2001).
- von Neumann, J., & Morgenstern, O. (1947). *Theory of games and economic behaviour* (2nd ed.). Princeton University Press.
- Wagner, R. E. (2012). Bailouts and the potential for distortion of federal criminal law: Industrial espionage and beyond. *Tulane Law Review*, 86 (5), 1017–1054.
- Western Region Security Office. (2001). *Notable industrial espionage cases*. https://www.wrc.noaa.gov/wrso/security_guide/industry.htm
- Whitty, M. T. (2021). Developing a conceptual model for insider threat. *Journal of Management & Organisation*, 27(5), 911–929. <https://doi.org/10.1017/jmo.2018.57>
- Yong, N. (2023, January 17). Industrial espionage: How China sneaks out America's technology secrets. BBC News.
- Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges, and opportunities. *Computers & security*, 104, paper no. 102221.
- Zatlin, J. R. (2008). Out of sight: Industrial espionage, ocular authority and east German communism, 1965–1989. *Contemporary European History*, 17(1), 45–71. <https://doi.org/10.1017/S0960777307004274>