Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Industrial espionage – A systematic literature review (SLR)

Tie Hou [a,*], Victoria Wang [b]

[a] School of Computer Science and Technology, Shandong Jianzhu University, Jinan, PR China
[b] Institute of Criminal Justice Studies, Faculty of Humanities and Social Sciences, University of Portsmouth, Portsmouth, UK

ARTICLE INFO

Article history:
Received 18 May 2020
Revised 31 July 2020
Accepted 23 August 2020
Available online 27 August 2020

Keywords:
Industrial espionage
Systematic literature review (SLR)
Key features
Challenges
Trends

ABSTRACT

Industrial Espionage (IE) is an umbrella term covering a complicated range of activities performed to gain competitive advantages, resulting in a huge amount of financial loss annually. Currently, techniques generated by rapid developments of Internet of Things (IOTs) and Data Science are enabling a massive increase of both frequency and power of IE related activities in our increasingly challenging global commercial environment. Thus, an in-depth understanding of IE is necessary. In this paper, we report a comprehensive Systematic Literature Review (SLR) of current English literature on IE. Particularly, we systematically: i) identify key features of IE by analysing its current definitions, and coin our own working definition; ii) discuss the current state of research on IE from different academic disciplines; iii) highlight some key challenges in the current state of research on IE; and iv) identify some possible trends in its future development. Further, based on our findings, we call for more multi-disciplinary/multi-agency research on IE in order to construct a comprehensive framework to combat IE.

1. Introduction

Most commercial research, by its very nature, is to gain a competitive edge. In the increasingly fierce global commercial competition, every organisation is faced with the issue of seizing extremely transient market opportunities to gain profit, market leadership, or even political power. The utilisation and protection of trade secrets and intellectual property are key to the success for enterprises. Currently, with the development of information technologies; especially Internet of Things (IoTs), big data and their related data science techniques, intelligence gathering becomes much easier, more powerful, and thus intensively competitive.

The intensive competitiveness, driven by high profits and propelled with advanced techniques, has resulted in many deviant and even criminal activities. Some of these activities, such as data breaches, are usually covered by the term of Industrial Espionage (IE). According to Verizon's annual Data Breach Investigations Reports (Verizon, 2019, 2018, 2017), most data breaches are committed with the intention of financial gain and espionage. In August 2016, Cybersecurity Ventures predicted that by 2021, the annual global cost of cybercrime will be more than $6 trillion, up from $3 trillion in 2015 (Cybersecurity Ventures, n.d.). This prediction stands still in its 2020 Official Annual Cybercrime Report (ibid.). Considering the extent of financial loss (among other commercial and legal damages), it is necessary to distinguish unacceptable business practices from acceptable ones by clarifying the two much-debated business practices of Industrial Espionage (IE) and Competitive Intelligence (CI).

* Corresponding author.
E-mail addresses: houtie2017@sdjzu.edu.cn (T. Hou), victoria.wang@port.ac.uk (V. Wang).
https://doi.org/10.1016/j.cose.2020.102019
0167-4048/

Both terms – Industrial Espionage (IE) and Competitive Intelligence (CI) – do not have standard definitions. These are defined differently by different individuals under the influence of various factors. For many, legality and ethics are the two key factors (e.g., Androulidakis and Kioupakis, 2016; Vashisth and Kumar, 2013; Jameson, 2011; Rothke, 2001; Kovacich, 2000). Illegal intelligence gathering activities are covered under the umbrella term of IE; whereas legal and ethical ones are covered under the umbrella term of CI. For example, Black's law dictionary (Garner, 2004) defines IE as one company's spying on another to steal trade secrets or other proprietary information; whereas the Strategic and Competitive Intelligence Professionals (SCIP) (n.d.) – a CI professional and international organisation – defines CI as a systematic and ethical program for gathering, analysing and managing external information that contributes to the strategic management process in enterprises. To add more complexity, culture difference is a key factor that influences how intelligence gathering is viewed; and when conducting business with other cultures, individuals would naturally use means of intelligence gathering that are regarded as acceptable in their own cultures (Schwartz, 2012; Morris et al., 2000; Bonthous, 1994).

Further, individuals might even consider illegal means of information gathering (defined by other, and even their own, nation-states) as acceptable since these means would benefit their own national/domestic entities (Trim, 2002). This could be escalated to the extent of considering IE as a convention (Solitander and Solitander, 2010) and CI as a euphemism for IE (Hill and Pemberton, 1995). To counter the convention, the SCIP has developed guidelines and a comprehensive code of conduct for all members to observe (SCIP, 2020 n.d.). Nevertheless, the boundary between CI and IE remains unclear in some extreme cases of CI, in which unethical information gathering still exists (Reinmoeller and Ansari, 2016; Crane, 2005; Wright and Roy, 1999). Thus, each legal case of IE costs both sides a significant amount of energy, time and money. For example, in 2006, Fakro – a Polish manufacturer of roof windows and accessories – started its complaint against Velux for unfair competition. More than a decade later, the European Commission rejected its complaint (European Commission, 2018). Again, in 2018, Uber settled with Waymo for 0.34% of Uber equity – about $244.8 million in stock – according to the Uber's $72 billion valuation (Toren, 2018).

Of course, the number of revealed industrial espionage cases are only the tip of an iceberg (Androulidakis and Kioupakis, 2016); and the actual financial cost is hard to be accurately estimated due to a number of factors. For example, in most cases, it takes months, even years, to be noticed by the victims (Verizon, 2018, 2014). Further, victims of industrial espionage are often extremely unwilling to report incidents; and tend to reach for out-of-courts settlements with their rivals (Toren, 2018; Waziri and Yerima, 2011; Crane, 2005). In this way, they could avoid the exposure of their incompetence and trade secrets, and thus the potential undermining of client and shareholder confidence (Reinmoeller and Ansari, 2016; Wright and Roy, 1999). However, the financial cost of IE could be estimated from various reports. For example, the Centre for Strategic and International Studies (CSIS) has published three reports to reveal the rapid increase in terms of financial damage of cybercrime and cyber espionage (Lewis, 2018; CSIS, 2014; Lewis and Baker, 2013). The Economic Impact of Cybercrime and Cyber Espionage 2014 report estimated that cybercrime and economic espionage could cost the world more than $445 billion annually (CSIS, 2014). Four years later, in its 2018 report, the estimation increased – by $100 billion – to be $545 billion (Lewis, 2018). Certainly, IE could result in not only direct but also indirect damages (e.g., future of the enterprises and stolen customers) (McKown, 2017) that are hard to estimate. Thus, it is unrealistic to count on legal measures to restore losses from industrial espionage; instead, awareness should play an important role in preventing activities of industrial espionage (Kahn, 2019; Spindell, 2013).

In this research, we review current literature available on Industrial Espionage (IE) to i) systemically analyse its key features in order to distinguish IE from CI; and ii) identify future research challenges in IE. Findings from the research would i) enhance business security, by promoting the development and application of data protection policies in terms of both business and client data; ii) provide an in-depth understanding of IE for researchers; iii) and encourage communications and collaborations on the research area of data security among key sectors, e.g., industry, commerce and academia. In this way, on the one hand, businesses would be able to strengthen their international competitiveness in the increasingly challenging global commercial environment. On the other hand, academic research and debates on IE will help to facilitate technological advancements, and good practices and techniques in security. The remainder of this paper is organised as follows. After this introductory section, Section 2 introduces our research methodology, i.e. Systematic Literature Review (SLR). Section 3 presents various definitions of IE in order to isolate its key features. Section 4 discusses the current state of research in the subject area; highlights some of the key challenges; and identifies some possible trends in its future development. Section 5 concludes this research and highlights some potential areas for further investigation.

2. Research methodology

In this research, we follow the guidelines proposed by Kitchenham and Charter (2007) to conduct our own Systematic Literature Review (SLR). In Kitchenham and Charter (2007), the general steps of the SLR methodology consist of three main phases: i) planning the review; ii) conducting the review; and iii) report the review. The tasks performed in each phase were described below.

2.1. *Planning the review*

The main goal of this SLR is to gather a thorough understanding of IE, including the current state of IE research and any unsolved challenges in the subject area. Therefore, the following research questions have been formulated to achieve our goal.

1) How is IE defined in existing literature?

Answering RQ1 could help to identify the common agreements and disagreements in existing definitions.

2) What are the key features that distinguish IE from CI?

Answering RQ2 can help to clarify these terms and to mitigate confusion.

3) Are there any special features of IE that make combating it difficult?

Answering RQ3 can help to recognize key challenges and suggest areas for further research.

Instead of analyzing an exhaustive collection of studies across numerous perspectives, we decided to focus on these that were closely related to the research questions. To this end, the literature search strategy was performed based on the following principles.

First, regarding the source of the literature, three online databases, Emerald Insight, Scopus and Springer were queried. Those databases were chosen due to their widely respected academic rigor and social impact. Further, references of the selected search results were examined to make sure that no study was missed. In addition, common internet search engines, e.g., Bing and Google, had been utilized to discover articles and government reports that were not indexed in digital libraries.

Secondly, it is crucial to define an appropriate scope and to identify key concepts. The combination of search strings used to identify relevant studies in the literature search were formulated as follows:

"industrial espionage" OR "business espionage" OR "corporate espionage"

OR "commercial espionage".

Thirdly, a set of inclusion and exclusion criteria was developed to ensure that only high-quality articles were included in this review. These inclusion criteria were:

1) Papers must be selected from journals, conference proceedings and book chapters;
2) Papers published between 2000 and 2020 were preferred; and
3) Papers must be clearly related to the research questions.

These exclusion criteria were:

1) Any paper not available to download was excluded;
2) Any paper not in English was excluded; and
3) Any preliminary paper of its already included complete version was excluded.

The process of literature evaluation was performed using the following criteria to ensure quality control:

1) The findings of a paper must provide a valuable contribution to the research questions, i.e. offering clarifications to existing debates in terms of definitions and understandings; raising new issues in current techno-social contexts; or proposing innovative suggestions;
2) The contents of a paper must still relevant and useful, especially considering the rapid development in technology and recent changes in relevant circumstance; and
3) A paper must not demonstrate any obvious bias that affects its reliability and validity, i.e. having a well-balanced source from a well-respected organisation with robust evidence to support its arguments; and stating clearly its contexts and limitations.

For example, in their paper 15 years ago, Desouza and Vanapalli (2005) investigated knowledge security protocols in five DIS (Defence and Intelligence Sectors) organizations. However, due to the rapid technological and social changes over the past 15 years, these data were no longer applicable. Therefore, their paper was excluded.

2.2. *Conducting the review*

The database search was conducted on 25 April 2020. The combinations of strings were searched in the title, keywords and abstract of all academic papers in the three online databases identified above. The searches led to the identification of 1310 papers, and those were entered into a Microsoft (MS) Excel sheet. The process of reference look-up identified an addition of 104 papers that was subsequently added to the MS Excel sheet. After elimination of duplicates, 1395 papers composed the initial data set to be analysed. Next, the set of inclusion and exclusion criteria was performed, resulting in a remainder of 117 papers. Further, 43 papers were removed based on our criteria to ensure quality control. Finally, 74 papers were identified as the final set of primary studies for this SLR. Of course, other papers befitting inclusion criteria 1 and 3 but were not published between 2000 and 2020, were used when necessary.

2.3. *Report the review*

The distribution of our selected previous research outputs, derived from their publication sources, is shown in Fig. 1. Most research outputs to be considered in this study were published in academic journals and conferences. Further, there were few outputs published in government and technical reports, books and book chapters.

The overview of the citation counts of the selected outputs are demonstrated in Fig. 2. The citation statistics were obtained through Scopus, Springer, ResearchGate, and Google Scholar. Out of the 74 selected previous research outputs, 63 were cited by other sources. Among these 63 outputs, only a few had more than 30 citations; whereas the rest had fewer than 30 citations, even none at all. Nevertheless, as the majority of the selected outputs were published in recent years, their citation rates are expected to increase.

3. What is industrial espionage?

As mentioned in the introductory section, the two much-debated business practices – Industrial Espionage (IE) and Competitive Intelligence (CI) – need to be clarified in order to distinguish unacceptable activities from acceptable ones. IE is an interdisciplinary subject without a standard definition (Button, 2020; Wimmer, 2015). As compared with IE, first

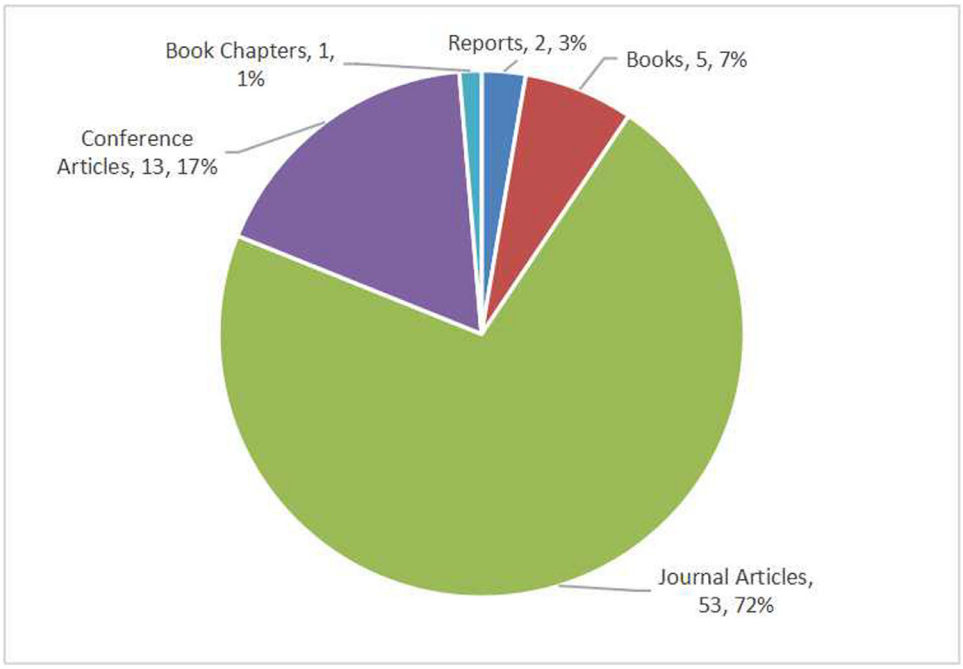

Fig. 1 – The distribution of sources of research outputs.

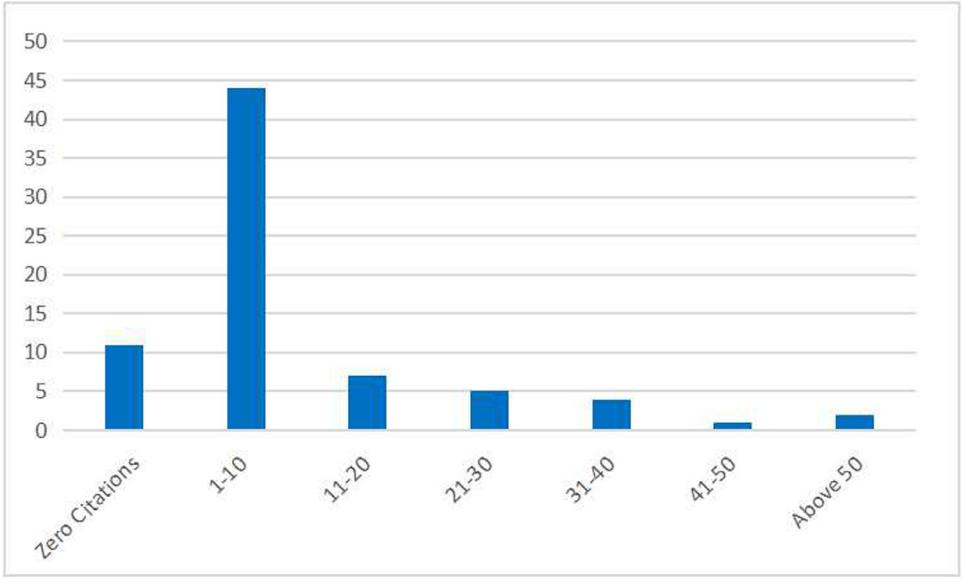

Fig. 2 – The citation counts of the selected outputs.

formally introduced in 1980 (Porter, 1980), CI is a more established concept. Yet, there are still contradicting views towards it among different researchers. For some, it is a slow developing and still relatively new research area in business (e.g., Priporas, 2019). For others, it is one of the fastest growing fields in the business world (e.g., Plessis and Gulwa, 2016).

Conceptually, CI can be considered both as a process and a product (Yin, 2018; Priporas et al., 2005). More specifically, it is a process that transforms ethically and legally collected information into actionable intelligence in order to obtain a competitive advantage to the enterprise (Pellissier and Nenzhelele, 2013; SCIP, n.d.). At the same time, it is also the final product of the process; simply put, the actionable intelligence about the external business environment (Yin, 2018; Muñoz-Cañavate and Alves-Albero, 2017). Aspinall (2011) divides CI into two types: i) human intelligence that is publicly unavailable intelligence gathered from human source (e.g., discussions with stakeholders); and ii) public intelligence that refers to intelligence that is accessible to the public (e.g., business reports, patents, media info, etc.).

For Boulouard et al. (2018), two key features that distinguish CI from IE are: i) the sources of information come from

environments that are external to businesses; and ii) the methods of information gathering are legal and ethical. Disagreeing with Boulouard et al. (2018), for Button (2020), IE utilizes both legal and illegal means. He lists a set of activities that are covered by the umbrella term of IE – from the least to the most in terms of illegality – these activities are: i) open source intelligence; ii) reverse engineering; iii) hiring employees of competitors; iv) dumpster diving; v) cultivating insiders; vi) illegal surveillance; and vii) hacking (ibid.). Of course, the list is useful. Yet, it is hard for any business to determine precisely the legality of any activities above, especially when dealing with an increasingly international and virtual business environment. Further, when the law fails to regulate complicated activities, ethical issues come into stage, making things even more muddled and confused.

All these have made defining IE very difficult and current definitions of it very much varied, thus hindering research in the subject area. Current definitions that are more relevant to the present research are conveniently set out in Table 1 below. Even these definitions are wide-ranging since they are coined based on different disciplinary contexts. As a result, some of these are too broad (e.g., economic espionage and CI); whereas others only focus on some specific features of IE.

Upon a careful review and analysis of the 15 current more relevant definitions of IE in Table 1, we have observed that every one of these definitions has at least emphasised one of the following four features. These are i) method; ii) intent; iii) actor; and iv) nature. Further, each of these conditions is derived from at least one of the current definitions in Table 1. Of course, since current definitions of Industrial Espionage (IE) are often confused with these of Competitive Intelligence (CI), in our derivation of these conditions, we have also used ideas in current definitions of CI. These four features with their conditions are:

1) **Method** – It is a process of systematically gathering, analysing and managing sensitive information, including trade secrets, operational information, intellectual property, etc., without permission of the owner of the information.
2) **Intent** – Its intention is to use the information acquired to i) gain competitive advantage; or ii) sell to interested individuals and/or groups.
3) **Actor** – It is usually conducted by an individual or an organization.
4) **Nature** – It qualifies as an illegal and unethical activity.

We have subsequently coined our own working definition of IE:

> An activity could only be considered as – Industrial Espionage (IE) – if and only if, for all four features of IE, each feature satisfies its own condition.

This working definition would work as a framework to guide our current examination of the current state of research on IE and identify its key challenges. Of course, this is only a working definition – an analytical construct – that serves its purpose in this particular context of research. It might potentially limit our scope of thinking, but based on the limited literature available, it is the best tool at the time of our research.

4. Research challenges

Globalization and new technology have revolutionised the methods used to perform activities of IE. In the past, IE makes use of methods, including theft of laptop and others, malicious software, electronic surveillance, corrupt practices (Sinha, 2012; Jones, 2008). Since the emergence of new technologies and devices (e.g., big data with AI, blockchain technologies, smart devices, etc.) the ways of perpetrating IE have been revolutionised (Camacho et al., 2019; Miller et al., 2018; Patel et al., 2017). However, resistance to change organisational policies and practices is a common phenomenon in today's business organisations, which leads to the formulation of organisational policies and practices always lagging behind the evolution of attacks (Greitzer et al., 2014a). Therefore, it is essential to examine the current state of research on IE; and identify its key challenges.

Next, we conduct such an examination from two main perspectives: i) human factors in IE; and ii) technical approaches in IE. Of course, the examination is linked to our working definition of IE with its four features in Section 3 above. In terms of *Method*, the feature extends to both human factors and technical approaches in IE, including various management techniques and IT design. Regarding *Intent*, it is mainly related to human factors. Of course, these human factors are deeply embedded in various technical designs of diverse intrusion detection/prevention software, e.g., insider attacker detection mechanisms. Concerning *Actor*, this feature is mainly associated with human factors of IE. Certainly, different actors would naturally adopt various technical approaches. Relating to *Nature*, as we have mentioned in the Introductory Section, culture difference is a key factor that influences perceptions of illegality and ethicality in terms of business practices (e.g., Schwartz, 2012). In this section, this feature is mainly discussed in association with our discussion of insiders. Unquestionably, varying perceptions of illegality and ethicality would naturally lead to different technical approaches and tools. More than ever, currently, obvious differences between local cultures, and thus illegality and ethicality are having significant impacts on businesses practices in different contexts globally. In Section 4.1.1 Insiders, we would touch on these as we discuss organisational culture as organisational culture arises from local culture/context (e.g., Vashisth and Kumar, 2013).

4.1. *Human factors in IE*

Human factors could be the weakest link in managing information security (Ashenden, 2018; Cheng et al., 2013) due to the complexity of human nature. Individual behaviour can influence many factors, such as security authentication and education, policies and procedures, and invasion techniques… Thus, the influence of human factors in IE is a multidisciplinary research area, which merits deeper exploration. Unfortunately, more focus has been given to technological approaches of IE; whereas little attention has been paid to human factors.

Table 1 – Key definitions in literature that are more relevant to this research.

Perspectives	Definitions	Citations
Business Ethics	"Industrial espionage is essentially a form of commercial intelligence gathering, usually, but not exclusively, on the part of industry competitors."	Crane, 2005, p. 233
Commercial	"Economic espionage (also government espionage) is a government's efforts to collect information, appropriate trade secrets, and steal knowledge (Nasheri, 2005). Industrial espionage is the same, but without direct government involvement."	Søilen, 2016, p. 52
Investigative	"…industrial espionage is generally defined as an individual or private business entity sponsorship or coordination of intelligence activity conducted for the purpose of enhancing their advantage in the marketplace."	The United States Federal Bureau of Investigations (FBI, xxx) cited in Kovacich, 2000, p. 326
Legal	"One company spying on another to steal trade secrets or other proprietary information."	Garner, 2004, p. 1651
Legal	"Industrial espionage refers to the clandestine obtaining of a company's trade secrets or other confidential information without permission and for nefarious motives."	Jameson, 2011, p. 290
Legal	"Industrial espionage is the same as economic espionage, except that rather than benefiting a foreign government, it benefits another private entity."	Wagner, 2012, p. 1040
Psychological	"Corporate espionage essentially describes illegal and unethical activities undertaken by organizations to systematically gather, analyse and manage information on competitors with the purpose of gaining a competitive edge in the market."	Vashisth and Kumar, 2013, p. 83
Risk Management	"Espionage is defined as the access to sensitive information without obtaining approval by the holder of the information (Crane, 2005). It is organized by foreign intelligence services (governmental espionage) or by corporations (industrial espionage) (Reisman, 2006) and it is executed by human experts (agents) in a specific target field that are able to distinguish between mundane information and information that is relevant for own organizational purposes (Kaperonis, 1984)."	Thorleuchter and Van den Poel, 2013, p. 3432
Security	"the use of, or facilitation of, illegal, clandestine, coercive or deceptive means by a private sector entity or its surrogates to acquire economic intelligence".	Porteous, 1994 cited in Holmström, 2010, p. 21
Security	"Generally speaking, however, the terms "industrial espionage," "economic espionage," or "corporate espionage" are all used when spying is conducted for commercial or business purposes and not purely national security purposes. Economic espionage is often used to refer to spying conducted or orchestrated by governments and it is usually international in scope. The terms industrial or corporate espionage are more often more intra-national and occur between companies or corporations who are competitors. Business espionage can include both sectors when the government is directly involved in the business sector, and, again, this happens in many places around the world."	Wimmer, 2015, p. xiv
Security	"Unlike the "traditional" espionage that is conducted for national security purposes, the practice of collecting confidential information without authorization from its owner for commercial or financial purposes is called industrial, corporate, commercial, or economic espionage."	Androulidakis and Kioupakis, 2016, p. v
Security Management	"…industrial espionage is undertaken by companies that 'are incapable of competing in a straightforward, normal manner'."	Trim, 2002, p. 7
Security Technology Research	"Industrial espionage, also known as corporate or business espionage, is spying that is conducted for commercial rather than national security purposes. However, it may be carried out by governments, companies and by other types of private organizations such as pressure groups. In the most straightforward cases, it is corporations spying on competitors to gain a market advantage, which probably entails the theft (or copying) of trade secrets and/or confidential or valuable information for use. In less commonly reported or understood scenarios, it may be a government spying on a corporation to gain information that will be of benefit to its own national military, industrial or commercial base."	Jones, 2008, p. 7
Technological	"Industrial espionage in the high-tech environment may be either focused on gaining information relating to a particular organization or may be a more general collection of useful corporate information that can be sold to interested groups or individuals."	Sutherland and Jones, 2008, p. 3
US government	"Industrial espionage is defined as activity conducted by a foreign government or by a foreign company with direct assistance of a foreign government against a private US company for the purpose of obtaining commercial secrets. This definition does not extend to activity of private entities conducted without foreign government involvement, nor does it pertain to lawful efforts to obtain commercially useful information, such as information available on the Internet. Although some legal actions may be a precursor to clandestine collection, they do not constitute industrial espionage."	Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (NCSC, 2000)

4.1.1. *Insiders*

The easiest way to capture a strong fortress is from within; and an insider could be anyone who has access to assets and/or sensitive information of the targeted organization. Almost 85% of cases of espionage are committed in cooperation with insiders (Dokko and Shin, 2019; Wright, 2017).

Combating insider threats requires the incorporation of different aspects involving individuals, technologies, and their related environments. It is not easy to create such an effective and coherent cyber ecosystem to detect, monitor and mitigate insider risks. The complexity of insider threat research requires a series of theories and approaches, including threat modelling; enterprise security policy and architecture; human governance strategies; insider vulnerability assessment; and security awareness; etc. (Omar, 2015; Al Hogail and Mirza, 2014; Brancik and Ghinita, 2011).

Methods of both behavioural analytics and technological measures are active areas in insider threat research. These methods include, for examples, personality traits (Greitzer et al., 2014b); data-centric threat detection combined with continuous monitoring of an intellectual property repository with advanced behavioural analytics (Warren, 2015); percolation model of a rule-based working environment to examine activities of normal individuals and insiders (Kepner et al., 2015); and human governance mechanism, such as organizational ethical climate and information security culture (Wong et al., 2019).

Vashisth and Kumar (2013) assert that unethical behaviours of insiders could be influenced by personality characteristics (e.g., having unmet goals, money problem, lack of loyalty, ideology, compromise, ego strength, and field experience); organisational and societal factors (e.g., leadership, reward systems, codes of conduct and norms, and culture); the interaction between individual factors and situational factors within organisations (e.g., reinforcement, obedience to authority, responsibility for actions, role taking); and the social interactions within the organisation (e.g., who are close to unethical actors will behave unethically). Subsequently, these psychological approaches could be used to assess the probability and quality of insider threats – "individuals are neither good nor bad but have the potential for both under the right circumstances" (Vashisth and Kumar, 2013, p. 86). Further, ethics should be deeply embedded in organisational cultures and policies to reduce the risk of IE.

Ho and Warkentin (2017) identify three key challenges in current insider threat research. These are: i) lack of an adequate theoretical framework to collect real-time behavioural data; ii) evidence of imperceptible insider threat activities is typically hidden and hard to collect; and iii) no reliable method or instrument to study the trustworthiness of privileged users. To respond to these challenges, they have conducted an experimental design using online games to simulate an insider threat scenario for predictive behavioural research (Ho and Warkentin, 2017). Differing from Ho and Warkentin's work relying on trustworthiness of spies, Rizzo et al. (2018) use behavioural measures, such as emotional indicators, to detect betrayers after the act of betrayal.

In terms of human factors in IE, most studies are carried out in psychology. Thus, previous research on insider threat from technical measures is very limited. Zhang et al. (2018) apply an unsupervised deep learning network model using the behaviour logs of insiders to improve the detection rate of insider threats. There are also calls for work from other perfectives. For example, Lee et al. (2020) point out that besides studies on insider threats to information systems, more research is needed to improve the professional expertise of police investigators to effectively deal with cases of IE.

4.1.2. *Techniques to combat computer crime*

Techniques applied as useful supplements have been adopted into countering IE from the fields of criminal profiling and digital evidence discovery.

In terms of criminal profiling, IE related research is very limited. Lee (2015) proposes that techniques of behavioural and investigative data profiling can be applied to identify i) the source of information leakage; and ii) deterrent effects of the subsequent legal actions that can help to prevent future IE related activities. Nevertheless, empirical evidence had demonstrated that the accuracy of results of criminal profiling is only about 75% (ibid.). At the time of conducting this review, no subsequent research has been found in this area.

Approaches in digital forensics can be modified into practical methods; and subsequently used by Incident Response Teams of organisations to deal with information security issues (e.g., Dokko and Shin, 2019; Chu et al., 2016, 2011). Jiang and Li (2019) discover that since 2013, digital forensics researchers have been focusing on cloud computing, IoTs, big data, and construction of the automatic, efficient and intelligent forensic system to produce better techniques. Currently, the tools and technologies in the field of digital forensics are means to fit within the IoT infrastructure, ameliorating issues caused by this infrastructure. These include huge volumes of data; heterogeneous data formats; diversity of devices; low computational capability; the application of encryption technology; the complexity of cloud storage; and limitations of laws and regulations (Alenezi et al., 2019; Basuchoudhary and Searle, 2019; Jiang and Li, 2019; Scanlon et al., 2015).

Of course, further research is required to improve the tools and techniques. For example, Luciano et al. (2018) point out that existing cyber forensics tools are highly impractical, and incapable of adapting to changes and evolution of technology in the industry. This is due to the fact that cyber forensics often involves the collaboration of multiple disciplines, which requires the creation of standardized criteria, especially in terms of the development and application of policies, ethics and tools (ibid.). Nevertheless, multi-disciplinary/multi-agency working requires the sharing of information, which could be problematic. For example, Alenezi et al. (2019) appeal against the sharing of information and experience on anti-forensics techniques from private sectors and governments, since a well-established anti-forensics data pool would naturally enrich the knowledge on tactics and measures used by cybercriminals and attackers, and thus potentially hampering computer investigations.

4.1.3. *Management and administration*

In theory, any organization should have a guidance for IE countermeasures covering all its business activities, transactions, and operational methods (Sinha, 2012). However,

establishing any appropriate and effective guidance is challenging. For example, when examining the rhetoric of Starwood's confidentiality agreement and its code of business conduct exposed in an IE lawsuit in which Starwood Hotels sued Hilton Hotels, Jameson (2011) points out that its employment agreement is written by lawyers to protect the interests of the corporation, thus it emphasizes narrowly its own self-interest. By contrast, the company's own publicized 'code of ethics and business conduct' contains much broader ethical values to inspire employees. Jameson (2011), thus, points out that enterprises should adopt a consistent ethical stance in their espoused and enacted ethical values, and raises the two key questions as follows:

1) What can be done to minimize the sharp contrasts between ethical values of one enterprise?
2) What if it is clearly written in the employment agreement regarding the prohibition of information leakage from employees, and the use of improperly obtained information about competitors?

Harrer and Wald (2016) state that enterprise security, concerned with the physical integrity, health and survival of employees, is an essential component of management control, but it is often ignored. Consequently, the development of management control systems in enterprise security remains a significant challenge due to a serious lack of research and innovation.

Socio-technical methods, which analyse relationships between people and technologies in the design of organizational systems, could be better means to prevent and cope with insider threats (Sadok et al., 2020). This is because IE tends to be cyber-enabled, resulting in the limitation of technical security solutions.

4.1.4. *Online social network*

Many enterprises increasingly deploy public communication channels for their employees to connect and interact with one another, but information security threats to organizations exposed by employees' Online Social Networks (OSNs) usages are unheeded (Liu and Bakici, 2019; Alimam et al., 2017). Braun and Esswein (2013) classify the identified corporate risks in OSNs; and analyse their properties and interdependencies in a risk catalog. Of course, as they stated that the catalog does not cover all risks, and thus needs to be extended to include, for three examples, i) counteractions of risks; ii) key figures for single risk factors; and iii) real benefits of implementing OSNs security control in enterprises (ibid.).

More recently, Ekandjo et al. (2018) point out that the following inabilities might be challenging for organisations to encounter:

i) to draw a line between private and professional roles;
ii) to influence employees to behave securely when using OSNs;
iii) to control what employees do on OSNs outside the office; and
iv) to balance the use of OSNs and the need for robust information security.

They further state that future research should be dedicated to how to best manage the risks of OSNs without restraining the positive side of OSNs usage.

4.2. *Technical approaches in IE*

A tremendous amount of technical approaches to protect intellectual property and confidential data are available, although they are probably not introduced originally to combat IE (e.g., Ahmad et al., 2019; Eckhart et al., 2019). Thus, the two key challenges to consider are:

1) How do the latest techniques impact upon IE in order to potentially mitigate its related issues?
2) Since no single approach could guarantee a complete immunity to IE, how should multiple approaches operate effectively with one another?

From a technical perspective, Androulidakis and Kioupakis (2016) provide a detailed discussion of means, equipment and tools to intercept conversations, data, and telecommunications in the framework of IE and its countermeasures. They state that effective protections against IE should involve: i) legal aspects (e.g., patents, trade secrets); ii) physical and IT security (e.g., equipment, software, and hardware); iii) IT governance (e.g., policies, roles, responsibilities, policy enforcement, auditing mechanisms); iv) financial restraints (e.g., budget); and v) training. Further, they argue that the factors affecting the effectiveness of a protection strategy, include: i) the availability of alternatives; ii) the kind and degree of protection on offer; and iii) cost and ultimate value of this protection to its owner (ibid.).

Recently, the application of blockchain has been proposed to resolve security and privacy related issues in the context of smart cities and digital economies. It has many advantages, such as securer data transference, and better anti-hacker encryption than any other existing deterrents that are suitable for working as a potential risk mitigation measure for IE (Parn and Edwards, 2019). Meanwhile, Makhdoom et al. (2019) address that there are various challenges faced by researchers in the secure adoption of blockchain in IoT. Thus, they call for more research on topics, including the lack of IoT centric consensus protocol; financial transaction validation rules; scalability; IoT device integration; protection of IoT devices against malware/remote code execution attacks; secure and synchronized software upgrade; secure privacy-preserving computations and data analytics; and integration of IoT communication protocols (ibid.).

Another interesting direction is to adopt artificial intelligence approaches to simulate and analyse espionage attacks, in order to enhance capabilities of intrusion detection and post event investigation. Parrend et al. (2018) present two main approaches for tracking unknown and complex cyberattacks – statistical analysis and machine learning. According to their survey, approaches of intrusion detection systems are moving from explicit expert rules and alert correlation proposals to data mining and behaviour tracking of individual entities of the IT system. They point out several core challenges in security investigation, including:

1) difficulties in determining how to operate cyber-threat intelligence inside of an organisation and how to deal with attackers who can access a similarly growing amount of information;
2) a lack of standard language to model abnormal behaviours; and
3) a lack of efficient tools to investigate highly encrypted traffic to avoid the loss of important critical information (ibid.).

Henningsen et al. (2018) argue that insider attacker detection mechanisms based on machine learning techniques in industrial wireless networks is a promising future research area. Trusted communications among the monitoring nodes play an important role in improving the accuracy of detection, which leads to in-depth considerations of various ideas, e.g., quantification and computation of trust and trust relationships.

5. Conclusion and further thoughts

In conclusion, we have provided a comprehensive review of current research in Industrial Espionage (IE). Particularly, we have coined a working definition of IE after identifying its key features; highlighted some key challenges after discussing the current state-of-the-art of IE research; identified some possible trends in its future development. We have called for multi-disciplinary and multi-agency collaborations among different academic disciplines, as well as academia, industry, and even governments, in order to establish more robust and ethical IE countermeasures, especially prevention standards and best practices.

We have indicated that IE as a research area is less established and multi-disciplinary. These two characteristics have naturally led to a number of challenges in terms of conducting research on IE, especially the following two:

1) **The lack of a standard definition.** Various terms, including: 'industrial espionage'; 'commercial intelligence'; 'competitive intelligence'; 'cyber espionage'; and 'economic espionage'… are frequently used interchangeably to describe a set of business practices that are highly varied.
2) **The lack of research collaboration.** IE related research projects tend to be conducted sporadically, and in disciplinary silos. Consequently, there have not been normative approaches critically analysing; and thus, building upon one another's work in the subject area. Hence, for researchers first approaching this subject, existing discoveries seem to be unconnected; and the subject area itself appears to be much muddled and confused.

A clear definition of IE is needed to avoid misunderstandings, and thus directing future research projects to a clearer trajectory. To this end, we have first clarified the two much-debated business practices of Industrial Espionage (IE) and Competitive Intelligence (CI) in order to distinguish acceptable practices from unacceptable ones. Subsequently, based on 15 current definitions of IE from various disciplines, we have identified four key features of IE including i) method, ii) intent, iii) actor, and iv) nature (each with its own condition); and subsequently coined a working definition of IE. An activity could only be considered as – Industrial Espionage (IE) – if and only if, all of its four features satisfy their conditions.

Methodologically, our comprehensive Systematic Literature Review (SLR) with its robust literature search strategy is necessary, since existing research projects on IE span across many disciplines, including Computer Science; Philosophy; Business and Management; Economics; Environment; Social and Political Sciences; Mathematics; Cultural and Media Studies; and History. Further, these projects seem to be conducted in isolated without any consideration of findings from previous research in other disciplines. We have also discovered that many proposed theories on IE are either with no proving, or being verified in specific conditions, such as a lab setting, a particular country, a specific company, etc. Nevertheless, in practice, strategies that are created in disciplinary silos without taking other factors – be they human or technological – into consideration are very likely to fail (cf. Tuptuk and Hailes, 2018).

Thus, in terms of future research, any research projects on IE, especially on possible strategies to combat IE, would need to i) cover both technological approaches and human factors; and ii) consider their related practical constraints. Hence, collaborations between academia and industry are required to verify performance efficiencies of theories in order to provide strategies that are ethically sound, efficient, robust, reliable, and cost effective. Further, preventative measures are more effective than post IE disaster recovery measures, since it is unrealistic to count on lawyers to recover losses from an IE; meanwhile, awareness plays a major role in protecting businesses (Kahn, 2019; Spindell, 2013). Thus, strategies to reduce the cost of implementing preventative measures need to be considered, especially in Small and Medium-Sized Enterprises (SMEs). In fact, Priporas (2019) claims that only large, multinational, and international enterprises conduct Commercial Intelligence (CI) activities in a professional fashion; whereas for the vast majority of enterprises, is an immature field – with many activities that could be considered as IE. This could be attributed to many obstacles, including low security awareness; inadequacies of formal education in CI; and financial difficulties (Priporas, 2019; Lee, 2014). Hence, multi-agency approaches, with financial and political supports from governments, are needed to overcome these obstacles; and thus, enabling the healthy development of businesses, especially SMEs (cf. Lee, 2014).

Therefore, we have called for more multi-disciplinary/multi-agency research on IE, especially these of an empirical nature, in order to: i) test existing theories widely in practice to verify the findings and insights; ii) identify potential interdependencies and complementarities in different IE related research areas; and iii) integrate various approaches that consider both technological approaches and human factors to construct a comprehensive framework in order to combat IE. In fact, collaborative research on IE is essential considering current increasingly rapid technological developments and challenging global commercial environment. Collaborative investigations are required to further explore potential roles of advanced technologies (e.g., blockchain, Artificial Intelligence (AI), Adversarial Machine Learning (AML)) in combating IE; as well as their related

legal/social/ethical implications in order to reflect both security and privacy. More than ever, multi-disciplinary/multi-agency research on IE is essential to illuminate better practices based on cultural and contextualised understandings of illegality and ethicality, as current differences in practices are having major impacts upon the process of globalisation.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Tie Hou: Conceptualization, Methodology, Writing - original draft, Resources. **Victoria Wang:** Conceptualization, Writing - review & editing, Methodology, Validation.

Acknowledgment

• This research was partially supported by the Shandong Jianzhu University Research Grant [XNBS1812] and the Shandong Provincial Key Research and Development Program (SPKR&DP) [2019GGX101068].

• This research was partially supported by the EPSRC project *Data Release - Trust, Identity, Privacy and Security* [EP/N028139/1; EP/N027825/1]

REFERENCES

Ahmad A, Webb J, Desouza K, Boorman J. Strategically-motivated advanced persistent threat: definition, process, tactics and a disinformation model of counterattack. Comput. Secur. 2019;86:402–18. doi:10.1016/j.cose.2019.07.001.

Alenezi A, Atlam HF, Alsagri R, Alassafi MO, Wills GB. IoT forensics: a state-of-the-art review, challenges and future directions. In: Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk. SciTePress; 2019. p. 106–15. doi:10.5220/0007905401060115.

Al Hogail A, Mirza A. Information security culture: a definition and a literature review. In: 2014 World Congress on Computer Applications and Information Systems. IEEE; 2014. p. 1–7. doi:10.1109/WCCAIS.2014.6916579.

Alimam M, Bertin E, Crespi N. ITIL perspective on enterprise social media. Int. J. Inf. Manag. 2017;37(4):317–26. doi:10.1016/j.ijinfomgt.2017.03.005.

Androulidakis I, Kioupakis FE. Industrial Espionage and Technical Surveillance Counter Measures. Springer International Publishing; 2016.

Ashenden D. In their own words: employee attitudes towards information security. Inf. Comput. Secur. 2018;26(3):327–37. doi:10.1108/ICS-04-2018-0042.

Aspinall Y. Competitive intelligence in the biopharmaceutical industry: the key elements. Bus. Inf. Rev. 2011;28(2):101–4. doi:10.1177/0266382111411070.

Basuchoudhary A, Searle N. Snatched secrets: cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets. Comput. Secur. 2019;87. doi:10.1016/j.cose.2019.101591.

Bonthous JM. Understanding intelligence across cultures. Int. J. Intell. Counter Intell. 1994;7(3):275–311. doi:10.1080/08850609408435251.

Boulouard Z, Koutti L, Chouati N, Haddadi A, Dousset B, Haddadi A, Bouhafer F. Visualizing large graphs out of unstructured data for competitive intelligence purposes. In: Proceedings of SAI Intelligent Systems Conference (IntelliSys) 2016. Springer; 2018. p. 605–26. doi:10.1007/978-3-319-56994-9_41.

Brancik K, Ghinita G. The optimization of situational awareness for insider threat detection. In: Proceedings of the First ACM Conference on Data and Application Security and Privacy. ACM; 2011. p. 231–6. doi:10.1145/1943513.1943544.

Braun R, Esswein W. Towards a conceptualization of corporate risks in online social networks: a literature based overview of risks. In: 2013 17th IEEE International Enterprise Distributed Object Computing Conference. IEEE; 2013. p. 267–74. doi:10.1109/EDOC.2013.37.

Button M. Editorial: economic and industrial espionage. Secur. J. 2020;33:1–5. doi:10.1057/s41284-019-00195-5.

Camacho J, García-Giménez J, Fuentes-García N, Maciá-Fernández G. Multivariate big data analysis for intrusion detection: 5 steps from the haystack to the needle. Comput. Secur. 2019;87 101603. doi:10.1016/j.cose.2019.101603.

Centre for Strategic & International Studies (CSIS). (2014). *Net losses: estimating the global cost of cybercrime*. McAfee. Retrieved from https://www.csis.org/analysis/net-losses-estimating-global-cost-cybercrime [accessed 16.05.20].

Cheng L, Li Y, Li W, Holm E, Zhai Q. Understanding the violation of is security policy in organizations: an integrated model based on social control and deterrence theory. Comput. Secur. 2013;39:447–59. doi:10.1016/j.cose.2013.09.009.

Chu HC, Deng DJ, Chao HC. An ontology-driven model for digital forensics investigations of computer incidents under the ubiquitous computing environments. Wirel. Pers. Commun. 2011;56(1):5–19. doi:10.1007/s11277-009-9886-x.

Chu HC, Yin MH, Hsu CH, Park JH. The disclosure of evaporating digital trails respecting the combinations of gmail and IE for pervasive multimedia. Multimed. Tools Appl. 2016;75(22):14039–55. doi:10.1007/s11042-014-2194-9.

Crane A. In the company of spies: when competitive intelligence gathering becomes industrial espionage. Bus. Horiz. 2005;48(3):233–40. doi:10.1016/j.bushor.2004.11.005.

Cybersecurity Ventures. The 2020 Official Annual Cybercrime Report; 2020 n.d.. Retrieved from https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ [accessed 16.05.20].

Desouza KC, Vanapalli GK. Securing knowledge in organizations: lessons from the defense and intelligence sectors. Int. J. Inf. Manag. 2005;25(1):85–98. doi:10.1016/j.ijinfomgt.2004.10.007.

Dokko J., & Shin M. (2019). A digital forensic investigation and verification model for industrial espionage. in *Digital Forensics and Cyber Crime. ICDF2C 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Springer 259, 128–146. 10.1007/978-3-030-05487-8_7.

Eckhart M, Meixner K, Winkler D, Ekelhart A. Securing the testing process for industrial automation software. Comput. Secur. 2019;85:156–80. doi:10.1016/j.cose.2019.04.016.

Ekandjo T, Jazri H, Peters A. Online social networks risks to organisations: a literature review. Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities. ACM, 2018.

European Commission. (2018). Case AT. 40026 Velux. Article 7(2) Regulation (EC) 773/2004. Retrieved from https://ec.europa.eu/competition/antitrust/cases/dec_docs/40026/40026_850_3.pdf [accessed 30.08.20].

Garner BA. Black's Law Dictionary. 8th Edition. Thomson West; 2004.

Greitzer FL, Strozer JR, Cohen S, Moore AP, Mundie D, Cowley J. Analysis of unintentional insider threats deriving from social engineering exploits. In: 2014 IEEE Security and Privacy Workshops. IEEE; 2014a. p. 236–50. doi:10.1109/SPW.2014.39.

Greitzer FL, Strozer J, Cohen S, Bergey J, Cowley J, Moore A, Mundie D. Unintentional insider threat: contributing factors, observables, and mitigation strategies. In: Proceedings of the 2014 IEEE 47th Hawaii International Conference on System Sciences. IEEE; 2014b. p. 2025–34. doi:10.1109/HICSS.2014.256.

Harrer J, Wald A. Levers of enterprise security control: a study on the use, measurement and value contribution. J. Manag. Control 2016;27(1):7–32. doi:10.1007/s00187-015-0210-5.

Henningsen S, Dietzel S, Scheuermann B. Misbehavior detection in industrial wireless networks: challenges and directions. Mob. Netw. Appl. 2018;23(5):1330–6. doi:10.1007/s11036-018-1040-0.

Hill LB, Pemberton JM. Information security: an overview and resource guide for information managers. Rec. Manag. Q. 1995;29:14–26.

Ho SM, Warkentin M. Leader's dilemma game: an experimental design for cyber insider threat research. Inf. Syst. Front. 2017;19(2):377–96. doi:10.1007/s10796-015-9599-5.

Holmström L. Industrial Espionage and Corporate Security: The Ericsson Case; 2010. *Reports of the Police College of Finland* 87/2010.

Jameson DA. The rhetoric of industrial espionage: the case of Starwood v. Hilton. Bus. Commun. Q. 2011;74(3):289–97. doi:10.1177/1080569911413811.

Jiang G, Li C. A scientometric review of research evolution in digital forensics. Proceedings of the 3rd International Conference on Computer Science and Application Engineering. ACM, 2019.

Jones A. Industrial espionage in a hi-tech world. Comput. Fraud Secur. 2008;2008(1):7–13. doi:10.1016/S1361-3723(08)70010-1.

Kahn R.A. (2019). Economic espionage in 2017 and beyond: 10 shocking ways they are stealing your intellectual property and corporate mojo. Business Law Today. Retrieved from https://www.americanbar.org/groups/business_law/publications/blt/2017/05/05_kahn/ [accessed 16.05.20].

Kaperonis I. Industrial espionage. Comput. Secur. 1984;3(2):117–21. doi:10.1016/0167-4048(84)90053-1.

Kepner J, Gadepally V, Michaleas P. Percolation model of insider threats to assess the optimum number of rules. Environ. Syst. Decis. 2015;35(4):504–10. doi:10.1007/s10669-015-9571-4.

Kitchenham B, Charters S. Guidelines for performing systematic literature reviews in software engineering. Evid. Based Softw. Eng. Tech. Rep. 2007.

Kovacich GL. Netspionage—the global threat to information, Part I: what is it and why i should care? Comput. Secur. 2000;19(4):326–36. doi:10.1016/S0167-4048(00)04020-7.

Lee CM. The strategic measures for the industrial security of small and medium business. Sci. World J., 2014 2014 Article 614201. doi:10.1155/2014/614201.

Lee CM. Criminal profiling and industrial security. Multimed. Tools Appl. 2015;74(5):1689–96. doi:10.1007/s11042-014-2014-2.

Lee S, Lee J, Jung J. An exploration of the necessary competencies of professional police investigators for industrial espionage cases in South Korea. Secur. J. 2020;33:119–38. doi:10.1057/s41284-019-00196-4.

Lewis, J. (2018). *Economic impact of cybercrime, no slowing down*. McAfee. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf [accessed 16.05.20].

Lewis, J., & Baker, S. (2013). *The economic impact of cybercrime and cyber espionage*. McAfee. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime-and-cyber-espionage [accessed 16.05.20].

Liu Y, Bakici T. Enterprise social media usage: the motives and the moderating role of public social media experience. Comput. Hum. Behav. 2019;101:163–72. doi:10.1016/j.chb.2019.07.029.

Luciano L, Baggili I, Topor M, Casey P, Breitinger F. Digital forensics in the next five years. In: Proceedings of the 13th International Conference on Availability, Reliability and Security; 2018. p. 1–14 Article No. 46. ACM. doi:10.1145/3230833.3232813.

Makhdoom I, Abolhasan M, Abbas H, Ni W. Blockchain's adoption in IoT: the challenges, and a way forward. J. Netw. Comput. Appl. 2019;125:251–79. doi:10.1016/j.jnca.2018.10.019.

McKown C. The American Greed Report: Corporate Spying Costs Billions, can It be Stopped?. CNBC; 2017. Retrieved from https://www.cnbc.com/2017/05/13/the-american-greed-report-corporate-spying-costs-billions-can-it-be-stopped.html [accessed 16.05.20].

Miller DB, Glisson WB, Yampolskiy M, Choo K-KR. Identifying 3D printer residual data via open-source documentation. Comput. Secur. 2018;75:10–23. doi:10.1016/j.cose.2018.01.011.

Morris DJ, Ettkin LP, Helms MM. Issues in the illegal transference of US information technologies. Inf. Manag. Comput. Secur. 2000;8(4):164–73. doi:10.1108/09685220010344916.

Muñoz-Cañavate A, Alves-Albero P. Competitive intelligence in Spain: a study of a sample of firms. Bus. Inf. Rev. 2017;34(4):194–204. doi:10.1177/0266382117735982.

National Counterintelligence and Security Center (NCSC). Annual Report to Congress on Foreign Economic Collection and Industrial Espionage; 2000. Retrieved from https://fas.org/irp/ops/ci/docs/fecie_fy00.pdf [accessed 16.05.20].

Nasheri H. Economic Espionage and Industrial Spying. Cambridge University Press; 2005.

Omar M. Insider threats: detecting and controlling malicious insiders. New Threats and Countermeasures in Digital Crime and Cyber Terrorism 2015:162–72. doi:10.4018/978-1-4666-8345-7.ch009.

Patel A, Alhussian H, Pedersen JM, Bounabat B, Celestino Júnior J, Katsikas S. A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems. Comput. Secur. 2017;64:92–109. doi:10.1016/j.cose.2016.07.002.

Parn E, Edwards D. Cyber threats confronting the digital built environment. Eng. Constr. Archit. Manag. 2019;26(2):245–66. doi:10.1108/ECAM-03-2018-0101.

Parrend P, Navarro J, Guigou F, Deruyver A, Collet P. Foundations and applications of artificial intelligence for zero-day and multi-step attack detection. EURASIP J. Inf. Secur. 2018;2018 Article number 4. doi:10.1186/s13635-018-0074-y.

Pellissier R, Nenzhelele TE. Towards a universal competitive intelligence process model. S. Afr. J. Inf. Manag. 2013;15(2):1–7. doi:10.4102/sajim.v15i2.567.

Plessis du, Gulwa M. Developing a competitive intelligence strategy framework supporting the competitive intelligence needs of a financial institution's decision makers. S. Afr. J. Inf. Manag. 2016;18(2):1–8. doi:10.4102/sajim.v18i2.726.

Priporas CV. Competitive intelligence practice in liquor retailing: evidence from a longitudinal case analysis. Int. J. Retail Distrib. Manag. 2019;47(9):997–1010. doi:10.1108/IJRDM-08-2018-0177.

Priporas CV, Gatsoris L, Zacharis V. Competitive intelligence activity: evidence from Greece. Mark. Intell. Plan. 2005;23(7):659–69. doi:10.1108/02634500510630195.
Porteous SD. Economic espionage: issues arising from increased government involvement with the private sector. Intell. Natl. Secur. 1994;9(4):735–52. doi:10.1080/02684529408432279.
Porter ME. Competitive Strategy: Techniques for Analyzing Industries and Competitors. New York, NY: Free Press; 1980.
Reinmoeller P, Ansari S. The persistence of a stigmatized practice: a study of competitive intelligence. Br. J. Manag. 2016;27(1):116–42. doi:10.1111/1467-8551.12106.
Reisman A. A taxonomic view of illegal transfer of technologies: a case study. J. Eng. Tech. Manag. 2006;23(4):292–312. doi:10.1016/j.jengtecman.2006.08.001.
Rizzo P, Jemmali C, Leung A, Haigh K, El-Nasr M. Detecting betrayers in online environments using active indicators. Lecture Notes in Computer Science 2018;10899:16–27 (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). doi:10.1007/978-3-319-93372-6_2.
Rothke B. Corporate espionage and what can be done to prevent it. Inf. Syst. Secur. 2001;10(5):1–7. doi:10.1201/1086/43315.10.5.20011101/31716.3.
Sadok M, Welch C, Bednar P. A socio-technical perspective to counter cyber-enabled industrial espionage. Secur. J. 2020;33:27–42. doi:10.1057/s41284-019-00198-2.
Scanlon M, Farina J, Kechadi T. Network investigation methodology for BitTorrent Sync: a peer-to-peer based file synchronisation service. Comput. Secur. 2015;54:27–43. doi:10.1016/j.cose.2015.05.003.
Schwartz MS. The state of business ethics in Israel: a light unto the nations? J. Bus. Ethics 2012;105(4):429–46. doi:10.1007/s10551-011-0975-x.
SCIP (n.d). Code of ethics for CI professionals. strategic and competitive intelligence professionals. Retrieved from https://www.scip.org/page/CodeofEthics [accessed 16.05.20].
Sinha S. Understanding industrial espionage for greater technological and economic security. IEEE Potentials 2012;31(3):37–41. doi:10.1109/MPOT.2012.2187118.
Søilen KS. Economic and industrial espionage at the start of the 21st century–status quaestionis. J. Intell. Stud. Bus. 2016;6(3):51–64. doi:10.37380/jisib.v6i3.196.
Solitander M, Solitander N. The sharing, protection and thievery of intellectual assets: the case of the Formula 1 industry. Manag. Decis. 2010;48(1):37–57. doi:10.1108/00251741011014445.
Spindell A. (2013). Industrial espionage threats to smes originate from within. *Thomas*. Retrieved from https://news.thomasnet.com/imt/2013/10/17/industrial-espionage-threats-to-smes-originate-from-within [accessed 16.05.20].
Sutherland I, Jones A. Industrial espionage from residual data: risks and countermeasures. In: Proceedings of the 6th Australian Digital Forensics Conference. Edith Cowan University; 2008. p. 167–72. doi:10.4225/75/57b2771540cc2.
Thorleuchter D, Van den Poel D. Protecting research and technology from espionage. Expert Syst. Appl. 2013;40(9):3432–40. doi:10.1016/j.eswa.2012.12.051.
Toren P. (2018). Some lessons from the waymo (alphabet) versus uber theft of trade secret litigation. *Ipwatchdog*. Retrieved from http://www.ipwatchdog.com/2018/02/14/waymo-uber-theft-trade-secret-litigation/id=93528/ [accessed 16.05.20].
Trim PR. Counteracting industrial espionage through counterintelligence: the case for a corporate intelligence unit and collaboration with government agencies. Secur. J. 2002;15(4):7–24. doi:10.1057/palgrave.sj.8340001.
Tuptuk N, Hailes S. Security of smart manufacturing systems. J. Manuf. Syst. 2018;47:93–106.
Vashisth A, Kumar A. Corporate espionage: the insider threat. Bus. Inf. Rev. 2013;30(2):83–90. doi:10.1177/0266382113491816.
Verizon. 2019 Data Breach Investigations Report (12th Edition); 2019. Retrieved from https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf [accessed 16.05.20].
Verizon. 2018 Data Breach Investigations Report (11th Edition); 2018. Retrieved from https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf [accessed 16.05.20].
Verizon. 2017 Data Breach Investigations Report (10th Edition); 2017. Retrieved from https://enterprise.verizon.com/resources/reports/2017_dbir.pdf [accessed 16.05.20].
Verizon. 2014 Data Breach Investigations Report; 2014. Retrieved from https://webfiles.dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf [accessed 16.05.20].
Wagner RE. Bailouts and the potential for distortion of federal criminal law: industrial espionage and beyond. Tulane Law Rev. 2012;86(5):1017–55.
Warren M. Modern IP theft and the insider threat. Comput. Fraud Secur. 2015;2015(6):5–10. doi:10.1016/S1361-3723(15)30056-7.
Waziri KM, Yerima TF. Industrial espionage and intellectual property rights protection: how legal is it legal. Int. J. Sustain. Dev. 2011;4(3):2011.
Wong W, Tan H, Tan K, Tseng M. Human factors in information leakage: mitigation strategies for information sharing integrity. Ind. Manag. Data Syst. 2019;119(6):1242–67. doi:10.1108/IMDS-12-2018-0546.
Wright L. People, risk, and security: How to Prevent Your Greatest Asset from Becoming Your Greatest Liability. Palgrave Macmillan; 2017.
Wright PC, Roy G. Industrial espionage and competitive intelligence: one you do; one you do not. J. Workplace Learn. 1999;11(2):53–9. doi:10.1108/13665629910260743.
Wimmer B. Business Espionage: Risks, Threats, and Countermeasures. Butterworth-Heinemann; 2015.
Yin C-Y. Measuring organizational impacts by integrating competitive intelligence into executive information system. J. Intell. Manuf. 2018;29(3):533–47. doi:10.1007/s10845-015-1135-4.
Zhang J, Chen Y, Ju A. Insider threat detection of adaptive optimization DBN for behavior logs. Turk. J. Electr. Eng. Comput. Sci. 2018;26(2):792–802. doi:10.3906/elk-1706-163.

Tie Hou is a lecturer in the School of Computer Science and Technology at the Shandong Jianzhu University. She received her PhD from the Department of Computer Science at the Swansea University in 2014. Her research interests mainly include logic, formal specification and verification, ontology reasoning and information visualisation.

Victoria Wang is a Reader on Security and Cybercrime in the Institute of Criminal Justice Studies, University of Portsmouth. Her current research ranges over cyber security and crime, surveillance studies, social theory, technological developments and online research methods. Her latest research projects involve: (i) techno-social theories as conceptual tools to understand cyberspace and its security issues; (ii) a general formal theory of digital identity and surveillance; (iii) formal methods for monitoring, data collection and interventions; (iv) cyberbullying; and (v) cyber security and crime in Nigeria and Vietnam, the criminal Darknet, and converged security threats and management measures in organisations. She has been exploring (i) the roles played by technology in social theories about modernity and (ii) the sociological nature of the technical and social development of the Internet. These studies have inspired the formulation of a theory of Phatic Technology - defined as technologies that establish, develop and maintain human relationships.