Security Journal (2020) 33:1–5
https://doi.org/10.1057/s41284-019-00195-5

EDITORIAL

Editorial: economic and industrial espionage

Mark Button[1]

Published online: 26 September 2019

In one of the most significant acts of industrial espionage ever, in the 1800s the British East India Company hired the botanist, Richard Fortune, to smuggle out of China tea cuttings, seeds, etc., which were used to help grow a tea industry in India which eclipsed the Chinese in a few decades (Rose 2010). Economic and industrial espionage are still significant problems for many countries and companies today; although techniques have moved on since Fortune disguised himself as a Chinese merchant, the spoils are this trade is still substantial.

The sizeable investments many companies make to develop intellectual property are lucrative targets for those willing to engage in such acts. Indeed, the head of MI5 (The UK Secret Service) revealed in 2012 how one UK company had suffered an £800 million loss from a state-sponsored cyber-attack in lost intellectual property and disadvantages in contract negotiations (Shah 2012). Indeed, the technological revolution of the last two decades has provided many more opportunities to pursue such acts, for both state and corporate actors, which for some can be done without even setting foot physically in the country or firm's premises.

These 'crimes', however, in the already under-researched world of what is increasingly become known as 'economic crime' have experienced very little academic curiosity. This special edition seeks to fill a very small gap in that research, but most importantly shed a light on this subject that it is envisaged will stimulate the interest and attention of other researchers to this area. Before this editorial introduces the papers of this special edition, it is important and timely to introduce readers to this subject.

There is a lexicon of terms that are used to describe a variety of problems that are considered in this special edition, which often overlap. These include, but by no means all, 'economic espionage', 'industrial espionage', 'corporate espionage', 'cyber espionage', 'commercial espionage' and 'intellectual property crime' to name some. It is not the purpose of this section to embark on a tortuous discussion to draw out a definition. Rather, Wagner's (2012, p. 1040) definitions will be used as the foundations for this editorial and discussion:

✉ Mark Button
mark.button@port.ac.uk

[1] Centre for Counter Fraud Studies, University of Portsmouth, Portsmouth, UK

> 'Economic espionage refers to targeting or acquiring trade secrets from domestic companies or government entities to knowingly benefit a foreign state' and
>
> 'Industrial espionage is the same as economic espionage, except that rather than benefiting a foreign government, it benefits another private entity'.

Corporate and commercial espionage are essentially another term for industrial espionage. Cyber espionage distinguishes one of the common means for undertaking it and 'intellectual property crime' covers a broader field to also encompass the substantial trade in counterfeit goods. Industrial espionage will be the term used in this editorial, but this is not to exclude economic espionage as they are often difficult to distinguish where state/companies interests often overlap, such as in China.

The definitional issues always create a challenge in estimating the magnitude of the problem, but those few estimates that have been offered provide little doubt to the substantial size of this global problem.

The US Intellectual Property Commission (2017) estimated trade secret theft costs 1–3% of GDP, meaning that the cost to the $18 trillion U.S. economy was between $180 billion and $540 billion. In the UK an estimate of the cost of cyber crime suggested of the £27 billion, £7.6 billion could be attributed to industrial espionage, including £2 billion financial services, £1.2 billion aerospace and defence and £1.6 billion mining (Cabinet Office/Detica 2011). Cyber is only one means to perpetrate espionage, so this is an under-estimate.

Estimating costs is problematic, but even more difficult are estimating the number of incidents. Reported data as for many other crimes are flawed; primarily, many organisations are reluctant to report such incidents; some may not know they are victims and thirdly those that are reported, because of the complex legal foundations, are often counted against other crimes (theft, hacking, etc.). Incidence surveys are also rare and often cover only part of the problem (cyber-breaches for instance).

Industrial espionage is perpetrated by a wide range of both illegal and legal means. Figure 1 illustrates the descent into more clearly illegal activities that offenders can utilise.

Open source intelligence (trade shows, reports, publications, social media, photos, etc.) can be used, which if in the public domain perfectly legitimate. Hiring employees of competitors can also be a tactic, although this might breach contracts signed between employee and previous organisation. The so-called dumpster diving is another tactic, where the rubbish of an organisation is sifted for intelligence. Products if available may sometimes be purchased and reverse engineered. Tactics can also involve much more clearly criminal acts such as placing insiders to steal information: bribing or blackmailing insiders are other tactics. Some perpetrators may resort to illegal surveillance where rooms or devices are bugged. Finally, the increasing use of cyber in an inter-connected world has led to numerous new opportunities to hack systems and devices to secure the necessary information.

The headline numbers, however, have raised very little interest in political elites, until President Donald Trump. In running for election and in government,

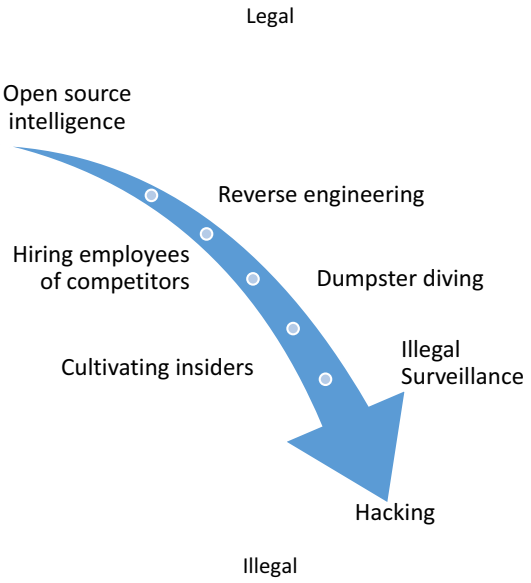

Fig. 1 Methods of industrial espionage

he has sought to raise the importance of the problem and pursue policy to try and address it. On the 28 September, 2011 he tweeted: 'China is stealing our jobs. We need to demand China stop manipulating its currency and end its rampant corporate espionage.'(https://twitter.com/realDonaldTrump/status/1191162435371130 88). In office he has pursued a trade policy, enforcement agenda among others to try and curb the problem. The UK and Europe are behind the US in tackling this problem with limited enforcement action and interest from senior politicians. For instance, a search through the speeches and announcements of the former British Prime Minister, Theresa May, at https://www.gov.uk/search/news-and-communications reveals nothing and only one brief mention in a wide ranging speech on emerging threats as Home Secretary in almost 9 years in office in those two senior roles.

This is not to say it is off the British Government's agenda, because the heads of both MI5 and GCHQ have both given speeches about the problem. In 2012, the head of MI5 warned corporate espionage was happening on an 'industrial scale' and in 2016 the head of GCHQ also warned British companies were experiencing 'industrial scale' cyber theft (Shah 2012; Whitehead 2016).

The general lack of interest of policy-makers, outside of the Trump administration and secret intelligence circles, does not therefore make it surprising when the lack of research into this subject is considered. There have been a handful of research monographs and practical guides published on the subject over the last 40 years by Heims (1982), Bottom and Gallati (1984), Cornwall (1991), Nasheri (2005), Hannas et al. (2013) and Roper (2013) to name the most significant. A brief search of Criminal Justice abstracts found 42 entries for 'industrial espionage', which compared to 869 for 'bribery' and 5608 for 'fraud', the latter of which are both seen as comparatively

under-researched areas of criminology (Levi 2016). These are not definitive figures of research, but do at least illustrate the relative lack of interest in comparison.

The small body of research that has been conducted can also be supplemented by other research on issues which overlap with industrial espionage. Given the role of hacking via phishing and the insider risk, the threats of these for other forms of economic crime has led to a body of research (for example, Nurse et al. 2014; Gheyas and Abdallah 2016; Phishme 2016; Goel et al. 2017). But these are not generally written from an industrial and economic espionage perspective, although many of their insights are useful. This edition, however, will seek to take a small step in filling this gap in research.

There has been little systematic research investigating the profile of those who engage in industrial espionage, how they undertake it and the outcomes of such cases, among many other issues. Knickmeier's paper is based upon a significant research project undertaken largely in Germany, but also covering parts of the EU. She provides some of the first data on the number of reported cases in Germany and Switzerland, the profile of those engaged in industrial espionage and their means of conducting it in Germany. She also provides some data on what happened in those cases in terms of investigation.

The insider and the human element is a very important factor in industrial espionage occurring. Sadok et al. in their paper offer insights on designing a socio-technical system within in an organisation to reduce the risk of insiders pursuing behaviours that exacerbate the technical risks. This then leads to Bederna and Szadeczky paper, who examine the use of botnets in cyber espionage. Botnets—which are usually more associated with denial of service attacks—and their role in espionage, particularly by some state backed organisations, are explored by them too.

The law covering industrial espionage is complex and intermingled with other crimes and civil torts. It is also subject to a degree—albeit weak—of international governance. Rowe's paper explores some of this international framework, as well as providing a detailed assessment of relevant US legislation. The paper also explores the significant challenges of dealing with state-sponsored espionage. In the penultimate paper, Konopatsch explores the Austrian and Swiss experience of using the criminal law to tackle industrial espionage, exposing some of the limitations of the law. She also explores the important new EU Directive on the Protection of Trade Secrets and some of the implications for EU member states.

South Korea's leading role in technology industries has made it a frequent target for espionage and in the final paper by Lee et al. they illustrate the enforcement-driven approach to the problem. For example in 2017, 334 offenders were arrested in 140 cases; this is significant given the size of the country and the level of enforcement action in the USA, Germany, Austria, Switzerland and the UK which some of the papers in this edition reveal is much less in comparison. The paper offers some important insights on the skills required of police officers dealing with these types of cases.

This special edition provides a window on a security problem that is probably one of biggest icebergs in the field of 'economic crime', a huge problem to corporations and government, but much of it hidden for a variety of reasons, noted above and explored in some of these papers. It is the ambition that this special edition will encourage more to pursue research and scholarly activity on this important subject, which is clearly

needed to advance our understanding and develop security and legal solutions to better combat it.

References

Bottom, N.R., and R.R. Gallati. 1984. *Industrial espionage: Intelligence techniques and countermeasures*. Oxford: Butterworth.

Cabinet Office/Detica. 2011. The cost of cyber crime. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf. Accessed 19 Aug 2019.

Cornwall, H. 1991. *The industrial espionage handbook*, 95–98. London: Century.

Gheyas, I.A., and A.E. Abdallah. 2016. Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Analytics* 1(1): 6.

Goel, S., K. Williams, and E. Dincelli. 2017. Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems* 18(1): 22.

Hannas, W.C., J. Mulvenon, and A.B. Puglisi. 2013. *Chinese industrial espionage: Technology acquisition and military modernisation*. Abingdon: Routledge.

Heims, P. A. 1982. *Countering industrial espionage*. 20th Century Security Education.

IP Commission. 2017. The theft of American intellectual property: Reassessments of the challenge and united states policy.

Levi, M. 2016. *The phantom capitalists: The organization and control of long-firm fraud*. Abingdon: Routledge.

Nasheri, H. 2005. *Economic espionage and industrial spying*. Cambridge: Cambridge University Press.

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. 2014. Understanding insider threat: A framework for characterising attacks. In *2014 IEEE security and privacy workshops* (pp. 214–228). IEEE.

Phishme (2016) Enterprise Phishing susceptibility and resiliency report. Retrieved from https://cofense.com/enterprise-phishing-susceptibility-report. Accessed 19 Aug 2019.

Roper, C. 2013. *Trade secret theft, industrial espionage, and the China threat*. Boca Raton: CRC Press.

Rose, S. 2010. *For all the tea in China*. Westminster: Penguin.

Shah, S. (2012). Corporate espionage on 'an industrial scale' targeting the UK. Retrieved from https://www.computing.co.uk/ctg/news/2187123/corporate-espionage-an-industrial-scale-targeting-uk. Accessed 19 Aug 2019.

Wagner, R. E. 2012. Bailouts and the potential for distortion of federal criminal law: Industrial espionage and beyond. Tulane Law Review, 86(5), 1017–1055. Retrieved from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1923469.

Whitehead, T. 2016. Business suffering 'industrial scale' cyber theft, warns GCHQ head. Retrieved from https://www.telegraph.co.uk/news/uknews/law-and-order/12197993/Business-suffering-industrial-scale-cyber-theft-warns-GCHQ-head.html. Accessed 19 Aug 2019.