Resilience after corporate or industrial espionage

Maarten IJzermans[1] and Wietse van den Berge[2]

Corporate and industrial espionage might occur at corporations as soon as other actors have competing interests. This makes everyone with competing interests a potential spy. However, if a corporation wishes to limit the possible impact of espionage, relatively simple mitigating measures might help. A first step is acknowledging that espionage might happen and that the corporation is a potential target. A second step is a risk analysis which identifies critical means and processes and their vulnerabilities. Based upon this awareness and risk analysis, the corporation can develop policies for whom to allow access to confidential corporate information. Restraint in allowing access is in place here. Authorization to access confidential information should only be granted after no restrictions were found during a screening process. Still, theft of confidential corporate information cannot be fully excluded. Therefore, also a need exists to prepare for situations in which espionage actually has occurred. In order to create resilience after espionage, corporations need to develop contingency plans in advance, and conduct damage assessments and improve mitigating measures to avoid future espionage afterwards.

Corporate and industrial espionage

Media reported in April 2019 that Chinese spies had stolen corporate information from Dutch chip machine producing company ASML in 2015. The estimated damage of several hundred million euro[1] lead to skeptical questions in politics[2] and media alike.[3] Within a context in which Chinese telecommunication corporation Huawei might deliver equipment for a 5G network[4], questions focus on China and the Chinese.[5] Apart from the generalizing and oftentimes suggestive character of such questions, focus on China and the Chinese imply a decrease of attention for other – possible – perpetrators of corporate or industrial espionage. It is not just something China or the Chinese apply.[6] Corporate or industrial espionage originates primarily from competing interests, only partly from different nationalities, which makes everyone with conflicting interests a potential threat.

Espionage: Competition, collecting information, clandestine

The Netherlands' General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst; AIVD) defines espionage as 'other countries' activities by which they clandestinely collect information in and regarding the Netherlands and thus harm our interests.'[7] This definition illustrates the AIVD's focus on state actors. However, in reality espionage is not something only states conduct. A more generic definition of espionage is used by Amnesty International: '[C]ollecting confidential intelligence for military, political or economical purposes.'[8] This second definition emphasizes the importance of military, political and/or economic interests. Combining elements of both definitions shows three essential characteristics of espionage: (1) it takes place in a *competitive* context, (2) concerns collecting *confidential information*, (3) in a *clandestine* way.

[1] Director of Risk Management at Hoffmann Risk Management.
[2] Security Consultant at Hoffmann Risk Management.

In a reaction to the publications in several media outlets, ASML stressed not to have been a victim of industrial espionage by China, but to have been a victim of corporate espionage by its competitor XTAL.[9] According to that explanation, XTAL's commercial interest was conflicting with ASML's. By using ASML's confidential source codes, software, pricing strategies and confidential user manuals, XTAL was able to take over Samsung as a client from ASML.[10] The clandestine aspect was that ASML had not approved former employees to take confidential information to XTAL.

Corporate and industrial espionage: Commercial and state driven

American legal terminology implicitly splits economic espionage into two categories without actually using the labels: (1) corporate espionage, and (2) industrial espionage.[11] Corporate espionage concerns the criminal character of 'commercial theft of trade secrets, regardless of who benefits,'[12] whereas industrial espionage 'is directed towards foreign economic espionage and requires that the theft of the trade secret be done to benefit a foreign government, instrumentality or agent.'[13]

As mentioned above, ASML emphasized to have been victim of corporate espionage[14], by which XTAL spied upon ASML, maybe even initiated by former ASML client Samsung.[15] However, the accusation of ASML being victim of Chinese initiated industrial espionage is imaginable. According to that explanation, Chinese-based XTAL served as a means for China to gain confidential information from ASML. It makes sense due to a high level of Chinese state interference with its economy, combined with a high level of integration of military, political and civilian intelligence agencies.[16] The AIVD has indications that China tries to obtain high-tech knowledge to support demands of its developing economy.[17]

The spy case regarding ASML thus could be either corporate or industrial espionage. And perhaps even a combination of both. But corporate espionage is not limited to XTAL and industrial espionage is not limited to China. A plethora of actors conduct corporate and industrial espionage. Corporations[18] will need to take into account the possibility that espionage will take place within its own organization, in particular when the corporation is involved in research and development of new technologies. However, corporations can also become victim of espionage that attracts less publicity, for example employees that copy confidential information for their own benefit.

In practice the difference between corporate and industrial espionage is not that clear, as boundaries between public and private sector intelligence become increasingly blurred.[19] This article will focus on relevant trends, the risk of espionage for corporations – whether corporate or industrial –, and mitigating measures that corporations can implement with the aim to create resilience against espionage. The obvious problem when writing on espionage is its clandestine character: activities happen in secret, thus not all is known. When espionage is discovered, corporations often are aloof to disclose the case out of fear for their reputations and to invite other spies in.[20]

Trends: More, mobility, mentality

Corporate and industrial espionage take place within corporate environments that are subject to societal developments. Author Moisés Naím observes a society wide decay of power. According to Naím, settled organizations, whether they are corporations or governments, all undergo three developments: (1) the more revolution, (2) the mobility revolution, and (3) the mentality revolution.

The more revolution indicates that an increasing number of people inhabit the earth, making it increasingly difficult for governments to control the masses of people, thus losing control. The mobility revolution indicates that this large number of uncontrollable people has the opportunity to travel around more easily and more often. Finally, the mentality revolution points out that this large number of uncontrollable people, who travel around a lot, do not take things for granted anymore, thus undermining governments' and large corporations' former power of authority.[21]

These societal developments have impact on corporate and industrial espionage. Loss of authority and capabilities of states[22] and corporations[23] alike lead to outsourcing of specialist functions. Whereas authorities, in particular the military, used to control research and development directly, processes and knowledge have become too complex. Instead, specialist companies develop and control such complex processes and high-tech knowledge. A similar trend can be observed among corporations. This implies that confidential information can be found at (sub-) contractors, making these attractive targets for espionage.

More: Increasing number of people

The growing number of people around the globe have needs and to provide these needs, economies are developing. Economies that up till recently lagged behind Western economies, develop rapidly and thus have huge demands. To meet these demands, high-tech knowledge might be beneficial. If this knowledge can be obtained by corporate or industrial espionage, such economies might save money and have the necessary knowledge available more quickly than by conducting its own research and development.[24] Like other Western intelligence and security agencies, the AIVD warns for countries conducting industrial espionage for political and economical purposes.[25]

Some of the countries with developing economies are subject to economic sanctions. These sanctions mainly concern so-called dual-use goods. Dual-use goods have a civilian application, but might be used for military purposes as well. Examples include radio-active material that can be used for energy plants, but might be used for creating nuclear bombs too. Concerning dual-use goods, commercial interests of corporations might conflict with security. Corporations like to sell goods. However, due to security they are limited to do so. A similar conflict between commercial and security interests might apply with using contractors from abroad. From a commercial point of view foreign contractors might be cheaper or more capable. From a security point of view, this might lead to proliferation of confidential information.

Mobility: Easy travelling of people and information

Nowadays, a corporation's contractors originate from all over the globe. As the mobility revolution indicates, travel has become accessible for an increasing number of people, including people from developing countries. On the other hand, companies need to take into account that their own employees travel abroad more easily as well, perhaps taking with them confidential information on their laptops or smart phones.[26] Information does not even need physical equipment to travel; Saving information in the cloud or sending information by email or social media enables a sender to contact a receiver on any given computer with Internet access. That same digital access might be used by cyber spies to gain information. This might concern confidential information as well.

Mobility in a more figurative way enables people to switch jobs more easily.[27] Especially in modern economies, life long employment is no longer the standard. This implies that employees who have access to confidential information leave a corporation, possibly taking their knowledge to their own start up or to a competitor, as was the case at ASML according to the ASML interpretation.[28]

Mentality: Not taking things for granted

As more people have access to more information, they increasingly criticize authority, whether this concerns governments or corporations. Demonstrations against governments and activism against corporations illustrate this tendency. For corporations this implies that activists for example, might try to access confidential information to support their claims against the corporation. Internally, this might be relevant as well. Apart from employees who conduct corporate espionage for their own start up or for a competitor, employees might also conduct corporate espionage due to disappointment or frustration, with the aim to undo abuse or to publish the confidential information to damage the corporation as whistleblowers. One example of a whistleblower is an employee who out of boredom and disappointment decided to address abuse at Hong Kong and Shanghai Banking Corporation (HSBC) in 2011. HSBC for years ignored international banking regulations by allowing money laundering and terrorist funding. Information by the whistleblower initiated investigations by the American Central Intelligence Agency and the Federal Bureau of Investigations. Eventually HSBC had to pay a 1.92 billion dollar fine.[29]

Risk: Recruitment, legal travelers, cyber espionage

Either as a whistleblower or from a commercial aim, the so-called insider threat remains present within corporations.[30] Within the context of the more, mobility and mentality revolutions, the insider threat overlaps with corporate and industrial espionage. The latter two manifest themselves in three ways. These ways – the so-called *modi operandi* – concern: (1) 'traditional' espionage, (2) legal travelers, and (3) cyber espionage.

'Traditional' espionage evolves around gaining a long term position within a corporation to withdraw confidential information, usually by recruiting an employee. External people with a natural access to a corporation also obtain (confidential) information, although usually not in-depth. However, by collecting all information available via these so-called legal travelers and combining the information, a rather complete image can be constructed. The latest way by which espionage takes place is through the cyber domain.[31]

Most espionage nowadays seems to occur through cyber means. This leads some analysts to suggest that cyber espionage will eventually replace traditional espionage. They point at the large quantities of information available and the relative ease with which the information can be obtained. Also, information acquired via cyber espionage seems to be objective, it has an illusion of certainty. Still, the information needs to be verified by other sources and sometimes to be placed in a correct context, especially in times of manipulation of facts by fake news. This makes 'traditional' espionage and use of legal travelers important as ever before.[32] Therefore, the three modi operandi to collect confidential information are often applied in combination.

Recruitment: Exploiting insiders

Intelligence agencies traditionally try to recruit people within organizations they are interested in and who hold positions which enables them to provide confidential information. Recruitment might be based upon an individual's hunger for adventure, need for money[33], disappointment or frustration.[34] Sometimes, an individual simply needs friendship or attention and the recruiting intelligence officer is able to provide that need. Extortion is another example of how an individual might be recruited. Intelligence officers will scout for people who are susceptible for recruitment, which basically overlaps with the insider threat. A lot of psychology is involved and relations between an individual and an intelligence officer develop over time, which make these operations time consuming and therefore inherently inefficient.[35] However, sometimes no alternatives are available and therefore this kind of modus operandi is still widely used.[36]

Although no recruitment was involved, two examples illustrate companies' vulnerabilities with respect to insiders. A former employee of Dutch telecommunication company KPN was arrested in 2018. He had taken client information and blackmailed KPN by pretending to be a hacker, showing snippets of the information online.[37] In 1997, an engineer of shaving company Gillette was sentenced for theft of trade secrets and wire fraud, disclosing confidential information to the company's competitors out of anger at his supervisor and fear for his job.[38]

Legal travelers: Exploiting outsiders

Intelligence agencies can also make use of so-called legal travelers.[39] These are individuals who have natural access to confidential information, for example because they have to work on a project within an organization. Oftentimes these people will only be allowed access to snippets of confidential information. Upon arrival back, for example in their country of origin, these people will be debriefed by intelligence officers, who will combine all snippets of information to construct an overview.[40] Legal travelers might serve as reconnaissance for a recruitment operation, possibly scouting for vulnerable insiders to recruit.

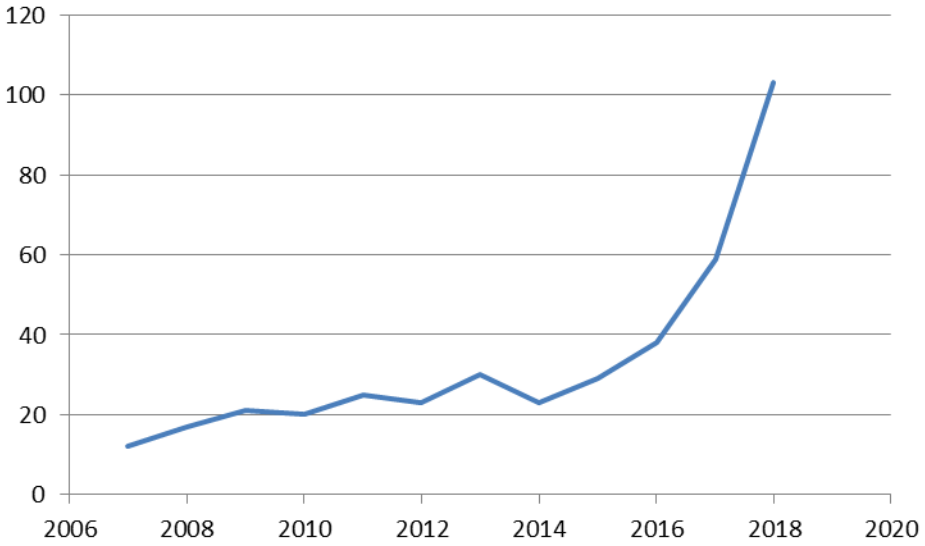
Along the indistinct line between using recruitment and using legal travelers, the mobility revolution provides opportunities to obtain confidential information in a quasi-legal fashion, for example by offering jobs to employees of competitors or by taking over companies that own interesting corporate information. An example concerns companies Waymo and Uber, both competing in developing self-driving cars: Waymo claims that former employee Anthony Levandowski secretly downloaded 14,000 files from Waymo's hardware systems before resigning a month later, and then used the information to launch the self-driving truck startup Otto. Uber eventually acquired Otto. Levandowski became responsible for all Uber's self-driving efforts.[41] Another example occurred in 1993, when eight executives left car company General Motors for its competitor Volkswagen. General Motors claimed they took confidential information and the case was settled by Volkswagen buying one billion dollars worth of General Motors parts and an additional one hundred million dollar.[42]

Cyber espionage: Exploiting digital vulnerabilities

Via digital means espionage might occur as well. Hackers might access single computers or entire networks that contain confidential information. Again, insiders might prove a vulnerability by

knowingly or unknowingly providing access codes or passwords. By methods such as social engineering, hackers try to exploit members or employees to gain information that they can use for their hack. Actually, '[c]yber attacks are the most used method that other nations, companies, and criminals employ to root out and steal your IP [intellectual property] and other valuable or sensitive information'[43] with an estimated loss of intellectual property in the United States alone worth 300 billion dollar per year in 2013.[44] The Center for Strategic and International Studies (CSIS) tracks significant cyber incidents since 2006, showing an increase from 12 incidents in 2007 to 103 in 2018.[45]

Figure 1: Graph indicating the increase in significant cyber incidents from 2007 to 2018, based upon numbers made available by CSIS.[46]



Examples of cyber espionage are manifold. In a combination of corporate and industrial espionage, British signals intelligence agency Government Communications Headquarters (GCHQ) spied upon Belgian communication company Belgacom – now Proximus – from approximately 2011 until around 2013. It provided GCHQ confidential information on clients of Belgacom, including Belgium based North Atlantic Treaty Organization and European Union.[47] A similar hack happened against Dutch-French SIM-card manufacturer Gemalto around 2010 and 2011 by GCHQ and American National Security Agency (NSA). This hack provided GCHQ and NSA insight in Gemalto's corporate information network.[48] In another example, Google acknowledged that a highly sophisticated cyberattack had occurred in December 2009, leading to theft of its intellectual property. Evidence suggested the hackers aimed to access the Gmail accounts of Chinese human rights activists. At the same time, financial, technological, media, and chemical companies were targeted.[49] Starting late 2009, hackers targeted computerized topographical maps from six American and European energy companies, including Exxon Mobil, Royal Dutch Shell, and BP, that locate potential oil reserves and were worth millions of dollars.[50]

Important to note here, and sometimes overlooked, is the fact that 'quite often, a cyber breach is possible because […] physical access was obtained beforehand, before the system could be compromised.'[51] The physical and cyber domains are more and more intertwined due to evolved technology, and are likely to be challenged interchangeably by converged threats, as vulnerabilities are exploited by the physical and cyber domain in conjunction. [52] This crucial realization is essential to

apply within the mitigating measures, that must be comprehensive and not only focusing on either physical or cyber vulnerabilities.

Mitigating measures: Awareness, 'need to know', screening

Whether another competitor company or country conducts corporate or industrial espionage respectively, is a decision that is taken by the other actor. Therefore, corporate and/or industrial espionage can never be fully ruled out. Realizing that corporate or industrial espionage can actually occur, is the first of three mitigating measures to limit the impact: (1) awareness, (2) apply 'need to know'-principle, and (3) conduct screening and verification.

Awareness that confidential information is vulnerable for corporate or industrial espionage poses the basis for the so-called 'need to know'-principle, which implies that only people who actually need the confidential information can have access to it. Before these people become authorized to gain access to the confidential information, it needs to be verified who they actually are and what their backgrounds are by screening. All mitigating measures aim to prevent spying activities, or else to disrupt or to detect them as soon as possible.

Awareness: Realizing vulnerability of confidential information

Employees of any corporation that has confidential information need to realize that corporate or industrial espionage might happen. Means or processes that somehow might be of interest to any other country, organization or individual are potential targets. These might include corporate processes, or newly developed products, but also client information, which might be of interest for an employee who is preparing a start up. Awareness that such confidential information poses a potential vulnerability should provide the basis for restraint in allowing access to it and lead to high responsiveness among employees with regard to suspicious situations. In order to decide what information might be interesting for others, it might help to '[t]hink like an attacker, not like a defender.'[53] Also, a risk analysis that identifies critical means and processes and their vulnerabilities might prove helpful here.[54]

'Need to know'-principle: Exclusiveness of confidential information

Confidential information should only be available to those employees who actually work with it. Individuals who do not work with the information on a daily basis, are not allowed access to the confidential information. This exclusiveness is known as the 'need to know'-principle. It manifests itself in compartmentalizing both physical and digital locations where confidential information is present. Only authorized personnel is allowed access there. Whenever unauthorized individuals (incidentally or occasionally) need access to the confidential information, authorized personnel will supervise them. When deemed necessary, this 'two person'-rule might be expanded to authorized personnel as well: in a location that holds confidential information, no one is allowed access alone.[55] Additionally, checks can be conducted whether specific items have been left or have been taken from the location, in particular audio or video equipment. Exclusiveness also includes communication systems, which need certified encryption, and forensic readiness regarding information technology.[56]

Screening: Verification of identity and background check

Before a corporation can authorize an employee, it needs to be verified that the respective employee is reliable. A pre-employment or in-employment screening provides verification of the actual identity of an individual and checks the individual's background. This background check assesses whether previous behavior or circumstances of an (candidate) employee might prove a risk with respect to the confidential information. A corporation might reconsider to hire someone who has close connections through family or friends with a competitor, due to the risk of corporate espionage. A screening sums up such risks, based upon which the corporation might decide to share confidential information with the individual, or not. However, circumstances might change, also after a screening. Therefore, in-employment screenings need frequent repetition.[57]

Resilience: Contingency plans, damage assessment, avoid repetition

Already in 2011 the Netherlands government acknowledged vulnerabilities of both government and corporations with regard to espionage:

> 'In order to increase awareness of the risks of espionage, […] organisations [need] to create insight into their key interests and the possible vulnerabilities of said key interests. This insight will enable organisations to be (even) better equipped to make their own decisions as to which measures they wish to implement in order to increase their resilience.'[58]

Focus lies primarily on prevention of industrial espionage.[59] However, corporate or industrial espionage cannot be fully excluded, only its impact limited. Corporations therefore also need to prepare for situations that corporate or industrial espionage has actually occurred in order to create true resilience, which is captured in three measures: (1) contingency plans, (2) damage assessment, and (3) avoiding repetition.

Contingency plans: Relevant 'what If'-scenarios

Preparations for incidents such as espionage can be written down in so-called contingency plans, that consider generic but realistic 'what if'-scenarios based upon risk analysis.[60] Although its contents depend on the issue at stake, most contingency plans at least consist of plans for redundancy, which deals with how corporate processes can continue as quickly as possible in a secure way, possibly from alternative locations by alternative means. Other elements in contingency plans are communication, both internally and externally, and perhaps legal issues. In case of corporate espionage a perpetrator for example might be sued for violating intellectual property.[61] Before such legal actions can be taken, making an inventory of what is lost is necessary.

Damage assessment: What is lost?

A corporation that has been the victim of corporate or industrial espionage needs to calendar what has been lost. For this, it is helpful if the organization has an up to date inventory of what it has available, in particular concerning confidential information. Accurate logging of who has which confidential information in possession is key here, forensic logging on digital networks as well. Only if it is clear what had been lost, investigation with the aim to retrieve the confidential information can be initiated. Another reason for assessing damage is that other stakeholders might be involved.

Perhaps clients need either to be informed that their information was lost too, or to be reassured that their information is still secure.

Avoid repetition: Repair vulnerabilities

Together with the damage assessment, vulnerabilities need to be repaired in order to avoid repetition. Both the victim corporation and its employees need to learn from the incident and develop improvements.[62] A danger after an incident is that a vulnerability might *seem* repaired as long as no other incidents occur. Then attention then is drawn away from the repairing process and no actual improvements in mitigating measures are implemented. Improvements need to be implemented and tested for effectiveness on a regular base.[63]

An example of what *not* to do was illustrated by Hewlett-Packard's scandal in 2006. Hewlett-Packard illegally spied on its own employees while trying to figure out the origin of boardroom news leaks and trying to avoid further leaks. Hewlett-Packard eventually had to pay over twenty million dollar to settle lawsuits.[64] Instead, a decent risk analysis should provide a basic framework on which to base security, including mitigating measures.

Concluding remarks

Espionage is referred to as the second oldest profession in the world[65], which illustrates how wide spread espionage is. Therefore, the current suggestion that corporate or industrial espionage is a threat originating from China is incomplete without adding that other countries, organizations or individuals might pose a threat as well. As soon as other actors have competing interests, they might want access to confidential information. Possibly, they use clandestine ways to obtain it.

The combination of competing interests, presence of confidential information, and clandestine ways to access it, makes almost everyone a potential spy. However, there is no need for panic. If an organization or corporation wishes to limit the possible impact of espionage, relatively simple mitigating measures might help. Awareness that corporate and industrial espionage might happen is a first start, especially when supported by a risk analysis which identifies critical means and processes and their vulnerabilities. The corporation then needs to develop policies regarding whom to provide access to the confidential information. Restraint in allowing access is in place here. Authorization to access the confidential information should only be granted after no restrictions were found during the screening process. During the screening, whether or not someone is Chinese, is not decisive; the interests at stake are. Still, espionage might occur. In such case, a contingency plan might prove helpful. Such plan with regard to espionage should initiate a damage assessment and start improvements in mitigating measures to avoid repetition.

[1] B. van Dijk and J. Leupen, 'Chinese spionnen stelen kostbare bedrijfsgeheimen van ASML', *FD*, 11 April 2019, https://fd.nl/ondernemen/1296245/chinese-spionnen-stelen-kostbare-bedrijfsgeheimen-van-asml.
[2] M. van Ast, 'Kamer wil bescherming tegen Chinese spionage: "Als we niet opletten, worden we leeggeroofd"', *AD*, 11 April 2019, https://www.ad.nl/politiek/kamer-wil-bescherming-tegen-chinese-spionage-als-we-niet-opletten-worden-we-leeggeroofd~a1027fb8/.
[3] 'Ask me anything', *BNR*, 11 April 2019, https://www.bnr.nl/podcast/ask-me-anything/10375043/bedrijfsspionage; 'Radio EenVandaag', *NPO Radio 1*, 15 April 2019, https://www.nporadio1.nl/radio-eenvandaag/onderwerpen/497829-meer-dan-200-000-chinese-spionnen-klopt-dat.
[4] C. Hawes 'Framing' Chinese Hi-Tech Firms: A Political and Legal Critique', *Australian Journal of Corporate Law*, 30 (1), 2015, pp. 34-57; M. Hijink, 'Huawei is nog 'te vaag' voor een veilig 5G-netwerk', *NRC*, 5 April 2019, https://www.nrc.nl/nieuws/2019/04/05/huawei-is-nog-te-vaag-voor-een-veilig-5g-netwerk-a3955866; 'The Huawei indictment tells a story of deceit and corporate espionage', *Washington Post*, 29 January 2019, https://www.washingtonpost.com/opinions/global-opinions/the-huawei-indictment-tells-a-story-of-deceit-and-corporate-espionage/2019/01/29/c2035abe-23f4-11e9-90cd-dedb0c92dc17_story.html?utm_term=.939a24e7c62b.
[5] 'Ask me anything', *BNR*; 'dr Kelder en Co', *NPO Radio 1*, 13 April 2019, https://www.nporadio1.nl/dr-kelder-en-co/onderwerpen/497628-de-chinese-roofmier-slaat-toe.
[6] M. van de Water, 'Jullie hebben geen idee van omvang Amerikaanse spionage in Nederland', *Volkskrant*,10 October 2013, https://www.volkskrant.nl/nieuws-achtergrond/jullie-hebben-geen-idee-van-omvang-amerikaanse-spionage-in-nederland~b41c08c7/. Also see: P.L. Mattis, 'Assessing Western Perspectives on Chinese Intelligence', *International Journal of Intelligence and CounterIntelligence*, 25(4), 2012, pp. 678-699.
[7] 'Jaarverslag 2018', *AIVD*, 2 April 2019, https://www.aivd.nl/documenten/jaarverslagen/2019/04/02/jaarverslag-aivd-2018, p. 8. Original in Dutch. Translation by the authors.
[8] Amnesty International, *Spionage en mensenrechten*, no date, https://www.amnesty.nl/encyclopedie/spionage-en-mensenrechten.
[9] 'ASML Disagrees with Implication of "Chinese Espionage"', *ASML* , 11 April 2019, https://www.asml.com/press/press-releases/asml-disagrees-with-implication-of-chinese-espionage/en/s5869?rid=58683; 'Samsung had rol bij spionage bij ASML suggereert topman ASML', *NOS*, 16 April 2019, https://nos.nl/artikel/2280789-samsung-had-rol-bij-spionage-bij-asml-suggereert-topman-asml.html.
[10] Van Dijk and Leupen, 'Chinese spionnen stelen kostbare bedrijfsgeheimen van ASML'.
[11] S. Brumley, 'The Difference Between Industry Espionage & Corporate Spying', *Chron*, no date, https://smallbusiness.chron.com/difference-between-industry-espionage-corporate-spying-76382.html.
[12] '1022. Introduction to the Economic Espionage Act', *United States Department of Justice*, no date, https://www.justice.gov/jm/criminal-resource-manual-1122-introduction-economic-espionage-act, codified at 18 U.S.C. § 1832.
[13] '1022. Introduction to the Economic Espionage Act', *United States Department of Justice*, codified at 18 U.S.C. § 1831.
[14] 'ASML Disagrees with Implication of "Chinese Espionage"', ASML.
[15] 'Samsung had rol bij spionage bij ASML suggereert topman ASML', *NOS*.
[16] B. Bereziuk, 'The Modus Operandi of Chinese Intelligence', *Researchgate*, 2016, https://www.researchgate.net/publication/319086489_The_Modus_Operandi_of_Chinese_Intelligence_A_Canadian_Perspective, p. 5.
[17] 'Jaarverslag 2018', *AIVD* , p. 9.
[18] As for corporations, most elements apply to (non-profit) organizations too.
[19] E. Lucas, 'The Spycraft Revolution', *Foreign Policy*, 27 April 2019, https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/.
[20] R.A. Khan, 'Economic Espionage in 2017 and Beyond: 10 Shocking Ways They Are Stealing Your Intellectual Property and Corporate Mojo', *American Bar*, 19 September 2018, https://www.americanbar.org/groups/business_law/publications/blt/2017/05/05_kahn/, p. 3,
[21] M. Naím, *The End of Power. From Boardrooms to Battlefields and Churches to States, Why Being in Charge isn't What it Used to Be*, New York: Basic Books, 2013, pp. 54-70.
[22] Ibidem, p. 123. This specifically concerns the military.
[23] Ibidem, pp. 181-183.

[24] Lucas, 'The Spycraft Revolution'.
[25] 'Jaarverslag 2018', *AIVD* , p. 8.
[26] Khan, 'Economic Espionage in 2017 and Beyond', p. 7.
[27] Ibidem, p. 10.
[28] 'ASML Disagrees with Implication of "Chinese Espionage"', ASML.
[29] M. Taibbi, 'Gangster Bankers: Too Big to Jail', *Rolling Stone*, 14 February 2013, https://www.rollingstone.com/politics/politics-news/gangster-bankers-too-big-to-jail-102004/.
[30] See: N. Catrantzos, *Managing the Insider Threat. No Dark Corners*, New York: CRC Press, 2012.
[31] Bereziuk, 'The Modus Operandi of Chinese Intelligence', pp. 5-6; Lucas, 'The Spycraft Revolution'.
[32] S. Grey, *The New Spymasters: Inside Espionage from the Cold War to Global Terror*, London: Viking , 2015. Also see: Catrantzos, *Managing the Insider Threat*, p. 9.
[33] G. Pols, 'Werknemer Siemens aangehouden op verdenking van bedrijfsspionage', *Volkskrant*, 7 April 2017, https://www.volkskrant.nl/economie/werknemer-siemens-aangehouden-op-verdenking-van-bedrijfsspionage~b5a11fad/.
[34] See: 'Famous Cases of Corporate Espionage', *Bloomberg*, 20 September 2011, https://www.bloomberg.com/news/photo-essays/2011-09-20/famous-cases-of-corporate-espionage.
[35] Lucas, 'The Spycraft Revolution'.
[36] Grey, *The New Spymasters*.
[37] 'Aanhoudingen in onderzoek naar digitale afdreiging KPN', *Politie Landelijke Eenheid*, 23 February 2018, https://www.politie.nl/nieuws/2018/februari/23/aanhoudingen-in-onderzoek-naar-digitale-afdreiging-kpn.html; 'Celstraffen geëist tegen afpersers KPN', *NOS*, 4 October 2018, https://nos.nl/artikel/2253366-celstraffen-geeist-tegen-afpersers-kpn.html.
[38] 'Famous Cases of Corporate Espionage', *Bloomberg*.
[39] The term 'legal travelers' is borrowed from K. Bruhn, 'Intelligence and Espionage (Denmark)', *International Encyclopaedia of the First World War*, 27 April 2018, https://encyclopedia.1914-1918-online.net/pdf/1914-1918-Online-intelligence_and_espionage_denmark-2018-04-27.pdf, p. 3. Legal travelers are described as 'tourists and business people who received instructions [of an intelligence agency] before departure and who were then debriefed on their return [for gathering intelligence]'.
[40] Lucas, 'The Spycraft Revolution'.
[41] A. Davies, 'Google Accuses Uber of Stealing its Self-Driving Car Tech', *Wired*, 23 February 2017, https://www.wired.com/2017/02/googles-waymo-just-dropped-explosive-lawsuit-uber-stealing-self-driving-tech/.
[42] 'Famous Cases of Corporate Espionage', *Bloomberg*.
[43] Khan, 'Economic Espionage in 2017 and Beyond', p. 1.
[44] Ibidem, p. 2.
[45] 'Significant Cyber Incidents', *CSIS*, accessed 8 May 2019, https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity. CSIS records significant cyber incidents since 2006, with an emphasis on cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars. Obviously, CSIS can only include the known cases.
[46] 'Significant Cyber Incidents', *CSIS*. Graph created by authors, based upon numbers made available by CSIS. The graph only includes full years, therefore leaving out both 2006 and 2019.
[47] M. Eeckhaut and N. Vanhecke, 'Britse geheime dienst bespioneerde jarenlang Belgacom-klanten', *De Standaard*, 13 December 2014, http://www.standaard.be/cnt/dmf20141212_01426880.
[48] 'Gemalto presents the findings of its investigations into the alleged hacking of SIM card encryption keys by Britain's Government Communications Headquarters (GCHQ) and the U.S. National Security Agency (NSA)', *Gemalto*, 25 Februari 2015, https://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx.
[49] 'Famous Cases of Corporate Espionage', *Bloomberg*.
[50] Ibidem.
[51] G. Kamp and J. Matthys, 'Bridging a governance gap: physical and cyber security', *Leiden Safety and Security Blog*, 26 March 2018, https://www.leidensafetyandsecurityblog.nl/articles/bridging-a-governance-gap-physical-and-cyber-security.
[52] Ibidem.
[53] Catrantzos, Managing the Insider Threat, p. 279. Original in italics.
[54] Ibidem, pp. 285-286. Also see: Khan, 'Economic Espionage in 2017 and Beyond', p. 5.
[55] Ibidem, p. 330.

[56] F.L. Wettering, 'CounterIntelligence: The Broke Triad,' *International Journal of Intelligence and Counter Intelligence*, Vol. 13, No. 3, 2000, pp. 265-300.
[57] Catrantzos, *Managing the Insider Threat*, pp. 285-286.
[58] 'The resilience of the government and business community against espionage is being increased', *Netherlands Ministry of Justice and Security*, 2011, https://www.government.nl/latest/news/2011/02/18/the-resilience-of-the-government-and-business-community-against-espionage-is-being-increased.
[59] 'Analysis of vulnerability to espionage', *AIVD*, 13 January 2011, https://english.aivd.nl/publications/publications/2011/01/13/aivd-analysis-of-vulnerability-to-espionage.
[60] Catrantzos, *Managing the Insider Threat*, pp. 265-266. Catrantzos applies the term 'strategic anticipation' instead of 'contingency plan'.
[61] For example in the Netherlands a victim whose confidential business information are stolen might receive compensation by the perpetrator. See: 'Wet bescherming bedrijfsgeheimen', *Overheid*, 22 October 2018, https://wetten.overheid.nl/BWBR0041459/2018-10-23.
[62] '5 lessons to be learned from the Gemalto NSA/GCHQ hack', *CBR*, no date, accessed 18 May 2019, https://www.cbronline.com/telecommunications/5-lessons-to-be-learned-from-the-gemalto-nsagchq-hack-4518001/.
[63] Catrantzos, *Managing the Insider Threat*, pp. 262-265.
[64] 'Famous Cases of Corporate Espionage', *Bloomberg*.
[65] A. Kouwenhoven, 'Spionage is één na oudste beroep ter wereld', *NRC*, 3 June 2014, https://www.nrc.nl/nieuws/2014/06/03/spionage-is-een-na-oudste-beroep-ter-wereld-1384504-a822162.