



Kluwer

a Wolters Kluwer business

*Gestolen geheimen,
verdamppte vermogens:
bedrijfsspionage in Nederland*

Ron Geeraets & Paul Koedijk

Programma

1. Introductie: terugblik in de spionagegeschiedenis
2. Doel van economische spionage
3. Welke informatie?
4. Welke verschijningsvormen?
5. Welke methoden?
6. Welke sectoren?
7. Hoe ontstaan risico's?
8. Wat zijn de gevolgen?
9. Van welke kanten komen de risico's?
10. Hoe de risico's te managen?



1. Inleiding: terugblik in de spionageschiedenis

- ❑ Periode van de Koude Oorlog:
 - Hoofdaccent op militair-strategische informatie
 - Bescherming vitale bedrijven (defensiegerelateerd)
- ❑ Na het einde van de Koude Oorlog:
 - Toenemende internationalisering/globalisering
 - Informatiemaatschappij : kennis als productiefactor
 - Geopolitieke verschuivingen; 'emerging economies'
- ❑ 'Economische wereldoorlog.': geen metafoor maar werkelijkheid
- ❑ Bescherming economische belangen als taak van I+V-diensten
- ❑ Verschuiving van accent op militaire informatie naar technologie en vervolgens naar economisch-civiel

2. Doel van economische spionage

- ❑ Informatievergaring
 - ❑ Verkrijgen van een (technologische) voorsprong
 - ❑ Concurrentie te slim af zijn
 - ❑ Economische schade toebrengen
- ❑ Directe schade toebrengen d.m.v. bijv. sabotage van bedrijfsprocessen, aantasting netwerken etc.
- ❑ Beïnvloeding van beslissingen
- ❑ Mogelijkheid creëren om (bedrijfs-) infrastructuur lam te leggen

3. Welke informatie?

- Verwerven van militaire informatie
- Verwerven van kennis massavernietigingswapens
- Verwerven van economische en technisch-wetenschappelijke informatie
- Verwerven van politieke en bestuurlijke informatie

(zie AIVD jaarverslag 2009)

3.A Marketing of spionage?

- ❑ Problemen bij de onderkenning van economische spionage
- ❑ Waar wordt marketing spionage?
- ❑ Grotendeels gelijksoortige informatiebehoefte
- ❑ Zachte en harde bedrijfsgeheimen

- ❑ Type informatiebronnen:
 - ❑ Open (70%)
 - ❑ Grijs (20%)
 - ❑ Illegaal (10%)

4. Welke verschijningsvormen?

- Benadering targets via agenten (humint)
- Digitale aanval
- Infiltratie
- Inzetten van een mol
- Inzetten van een slaper



5.A Welke methodes bij humint?

- Zeer divers en **veelkleurig**:
- Informatie stelen/inbreken: maskering als 'gewone' inbraak?
- Informatie vervalsen
- Infiltratie
- "Aanlopen"
- Omkoping
- Chantage
- Misleiding
- Inzet business cover facilitator
- Fysieke dreiging
- Pressie/afpersing
- Honey trap
- Verleiding in diverse vormen
- Ontvangen van uitnodigingen
- Etc. etc.

5.B Welke verschijningsvormen van humint?

Hoe presenteert een inlichtingenofficier of bedrijfsspion zich?

Antwoord: in vele kleuren en vormen doch vaak als:

- Diplomaat
- Zakenman
- Wetenschapper
- Student
- Journalist
- Sollicitant

5.C Welke methodes bij digitale spionage?

- Hacken PC's en Servers
- Phishing
- Kopiëren van bestanden op gegevensdragers
- Beïnvloeding
- Overname sturing PC's en Servers
- Achterlaten virussen, trojan horses, spy ware etc.
- Informatie uit open bronnen
- Besmette media, emails en websites
- Info via eigen websites en sociale netwerksites als hyves, facebook etc.
- Aftappen
- Uitluisteren
- Zoeken op trefwoorden
- Volgen internetgedrag
- Camera's en microfoons achterlaten
- Etc. etc.

6. Welke sectoren vormen het doelwit?

- ❑ Vanuit een optiek van informatievergaring:
 - ❑ Technologisch innovatieve sectoren
 - ❑ CBRN gerelateerde bedrijven en (semi-publieke) organisaties
 - ❑ CBRN gerelateerde wetenschap
 - ❑ Bedrijven uit het militair-industrieel complex
- ❑ Vanuit een optiek van sabotage, lam leggen infrastructuur en destructie:
 - ❑ Bancaire sector
 - ❑ CBRN gerelateerde bedrijven
 - ❑ Energie- en watersector
 - ❑ Transportsector (met name luchtvaart)
 - ❑ Veroorzaken grootschalige milieu-incidenten

7. Hoe ontstaan risico's?

- Gebrek aan security awareness (nummer 1!)
- In dienst nemen niet gescreend personeel
- Ontbreken systeem van integriteitsmanagement
- Ontbreken internetprotocol
- Ontbreken code of conduct
- Ontbreken of niet functionerend toegangsbeleid
- Ontbreken security managementsysteem
- Uitbesteden data bases, data onderhoud en server beheer
- Ontbreken systeem voor netwerkbescherming (tegen digitale aanvallen)
- Ontoereikende fysieke bescherming
- Etc. etc....

8. Wat zijn de gevolgen?

- ❑ Soms niet direct waarneembaar doch:
 - ❑ In potentie gigantisch
- ❑ Soms niet calculeerbaar
- ❑ *Daarnaast:*
 - ❑ Imagoschade
 - ❑ Op definitieve afstand worden gezet t.o.v. concurrentie
 - ❑ Faillissement
 - ❑ Politieke schade
- ❑ Maatschappelijke schade:
 - ❑ Banenverlies
 - ❑ Effect op handelsbalans
 - ❑ Verlies aan belastinginkomsten
 - ❑ Psychologisch effect op innovatiedrang

8.A Gevolgen voor Nederland

- ❑ Positie van Nederland in de wereld:
 - ❑ Knooppuntfunctie
 - ❑ Vijfde exporteur ter wereld
 - ❑ Lucratieve nichemarkten
 - ❑ Technologische vernieuwing
- ❑ Marktwaaarde ligt steeds meer in intellectuele eigendom
- ❑ Strategische informatie als financieel waardeerbare productiefactor
- ❑ Geschatte schade: 263 miljoen euro
- ❑ Houding tegenover bewaking van economische belangen
- ❑ Rol van BVD en AIVD: Nederland te braaf?
- ❑ Waarschuwingen door AIVD en MIVD

9. Van welke kanten komen de risico's?

- Overheden zoals bijv. China, Rusland, Iran, Midden-Oosten landen
- Bondgenoten! – Zoals:
 - GCHQ: 'protects GB's economic well-being'
 - SDECE
 - CIA
 - Private inlichtingendiensten
- Bedrijven met het profiel:
 - Veelal internationaal opererend en/of
 - Met een competitief belang en/of
 - Verwevenheid met nationale/lokale overheid
- Actiegroepen (milieugroeperingen, dierenactivisten, antiglobalisten, krakers etc.)
- Subversieve NGO's
- Terroristische groeperingen
- Eigen personeel
- Media/journalistiek

10. Hoe de risico's te managen?

- ❑ Uitvoeren risicoanalyse
- ❑ Maatregelen als spiegelbeeld van de risicoanalyse
 - Integriteitsmanagement waaronder screening van personeel
 - Kritisch zijn t.a.v. uitbesteding vitale functies
 - Security awareness en voorlichting
 - Bescherming informatie en telecommunicatiesystemen
 - Ontwerpen en implementeren security management systeem
 - Operational security t.a.v. niet-gerubriceerde informatie
 - Fysieke maatregelen
 - Eventueel contra-inlichtingen (CI)maatregelen

