Cyber Intelligence

Isodarco, Aug. 9, 2025

Bart Jacobs — Radboud University Nijmegen, NL
bart@cs.ru.nl

Overview

Cyber Intelligence

Where we are, so far

Personal interest/background in intelligence

- **Content reasons**
  - high societal interest — topic of national referendum in NL in 2018
  - internationally hot since Snowden revelations (2013)
  - high geo-political interest, with powerplay between nations
  - few lawyers know the topic — incomprehensible laws/practice
  - high CS content, about hacking, interception, big data, AI
  - quite a few CS students choose to work in intelligence
- **Professional roles**
  - member of NL intelligence review committee, in 2020
  - member of NL intelligence oversight knowledge circle, since 2015
  - occasional advice work on intelligence for NL Parliament
  - regular role as commentator in the media

Academic interest

- Fascinating and delicate topic: how to regulate secret state activities?
  - political philosophical perspective: republicanism, after Pettit et al
  - freedom as absence of (potential) domination
  - applies well in the digital domain — with big tech's domination
- Author of historical & legal articles on this topic, e.g.
  - on Maximator, north-west European version of Five Eyes, in *Intelligence and National Security*, 2020
  - on success of NL codebreaking in WWI, in *HistoCrypt 2024*

Some general remarks

- Intelligence & security organisations have as general aims to protect national security / democratic order / vital interests of the state
  - "national security" and "vital interests" offer ample space for interpretation
  - politisation is always a big concern / risk / danger: serving the people, not those in power
  - attitude of professionals: speaking truth to power
  - they should improve decision making by public authorities
- Intelligence has a strong national focus & tradition
  - for instance, EU laws do not apply to intelligence
- This presentation contains general points, which do not apply everywhere
  - there are many variations, e.g. in organisation of oversight
  - other differences e.g. w.r.t. economic espionage

Legal framework, very generally

- Intelligence & security organisations have exceptional powers
  - informally, to do everything that God has forbidden
  - impersonate, deceive, ly, falsify, steal, tap, hack, etc
- Their actions of must satisfy requirements of
  - necessity, to reach agreed-upon goals
  - proportionality, damage should be reasonable w.r.t. gains
  - subsidiarity, no easier, less damaging method can achieve the same
  - directedness, sometimes explicit, but part of proportionality
- Most countries have different protections for own and foreign citizens
  - not NL, but subsidiarity leads to different approaches
- Independent oversight is part of democratic control
  - e.g. by judges, institutional experts, parliament (or combinations)
  - in different phases, *ex-ante*, *ex-durante*, *ex-post*
  - European Court of Human Rights (ECHRM): *there must be end-to-end safeguards*

Organisational arrangements

- Some countries have separate services for internal / domestic and external / foreign
- Other countries distinguish civil versus military

Here most interest in sigint activities

- sigint = signals intelligence, in contrast to e.g. humint intelligence from human spies
- cyber activities are often integrated into sigint services

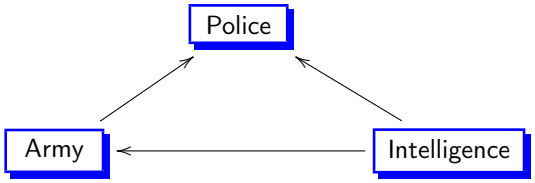
Some intelligence organisations

- USA
  - Internal: FBI, also with police tasks
  - External: CIA, traditionally mostly humint
  - Sigint: NSA $\geq$ FBI + CIA
- UK
  - Internal: MI5
  - External: MI6 (aka. SIS), traditionally mostly humit
  - Sigint: GCHQ $\geq$ MI5 + MI6
- GER
  - Internal: BfV = *Bundesamt für Verfassungsschutz*
  - External: BND = *Bundesnachrichtendienst*, humint & sigint
- Isr
  - Internal: Sjin Bet (Sjabak)
  - External: Mossad
  - Sigint: Unit 8200
  - Military: Aman
- NL
  - General: AIVD
  - Military: MIVD
  - Sigint: JSCU = Joint Sigint Cyber Unit (of both AIVD & MIVD)

Where we are, so far

iCIS | Digital Security
Radboud University

Three state-power organisations



The arrows indicate possible support. How many people work at these organisations?

- The police has internal (national) monopoly on the use of force
- The army has the external force monopoly — with threat posture
- The intelligence organisations (typically) cannot use force or arrest, but they have special investigative powers
  - Exemptions exist, e.g. in US (FBI) and Sweden (Säpo)

iCIS | Digital Security
Radboud University

About the police

Main tasks:

(1) Enforcing the law — esp. criminal law
  - under supervision of a state / public prosecutor (*officier van justitie*)

(2) Maintaining public order and safety
  - under supervision of the mayor (local government)

Special powers (highly regulated)

- physical coercion may be used to arrest & detain (freedom violating)
- investigative powers may be applied to suspects (privacy-violating)

Convictions

- done in public by an independent judge — open to appeal
- on the basis of evidence provided by the police, presented by an attorney, contested by a defense lawyer

iCIS | Digital Security
Radboud University

About the army

Main tasks

(1) Territorial defence
- nationally, and of allies (e.g. in NATO context)

(2) Maintaining international order and stability
- e.g. via UN peace keeping missions

(3) Assisting public authorities in emergency situations
- e.g. during a flood, pandemic, etc.

About digital warfare (think: stuxnet)

- Mostly done by intelligence services, under the radar
- There is NL *Cyber command*, active after "declaration of war"

About intelligence, in NL: offensive & defensive

AIVD main tasks

(1) Protecting the democratic order and national security
- including threat analysis, backgrond checks, defensive measures

(2) International investigations (spying) to learn hidden political agendas
- based on national priorities (*geïntegreerde aanwijzing*)

MIVD main tasks

(1) International investigations (spying), into military agendas/power

(2) Protecting own military power & secrets, against threats

Where we are, so far

Police versus intelligence; traditional difference

(1) The police operates in essence reactively
- only after someone has been murdered, investigations start
- they are focused, with selective data collection, in principle
- focus is on finding the perpetrator(s)
- "proportionality" of privacy-violations is relatively easy to judge

(2) Intelligence service operate proactively
- they seek to identify and evaluate threats
- investigations can be broad, with bulk data collection
- proportionality is hard to judge, e.g. all passenger data

Increasingly, the police is working more proactively, in data-driven investigations and in predictive policing
- this is somewhat sensitive / controversial and not well-regulated yet

What is intelligence good for?

(1) For well-informed decision-making
- esp. by relevant cabinet ministers: prime minister, foreign & internal affairs, justice, ...
- e.g. to expell foreign diplomats, to deploy military units, or to determine one's own negotiation position

(2) For preventing (terrorist) attacks or finding attackers
- actual arrests have to be done by the police
- on the basis of transferred "signals" (called *ambtsbericht* in NL)
- the police has to redo essentially all investigations
- intelligence info is secret and can thus not be used in court

(3) For disturbing attacks and preparatory activities
- intelligence services can disturb themselves, to some extent
- e.g. digitally or also physically, in exceptional cases
- or by warning people ("we are watching you!")

(4) Covert action, mostly part of aggressive, non-EU services

Where we are, so far

Phone/IP taps

- Phone tapping has a long history, well-established approach:
  - technically standardised, built into phone switches
  - also legally clear, based on authorisation by judge/DA/minister
  - applies to phone number(s) of inidividual, or to small group
- Basically the same approach applies to IP-taps
- All this is gone with end-to-end encryption (E2EE) of messaging apps
  - Whatsapp, Signal, iMessage, Telegram, ...
  - big frustration to law enforcement / intelligence
  - ongoing hot debate: legal demands, technical feasibility, organisational set-up, economic interests,

Bulk collections

- Obtained via fibre/satellite interception, hacking, informers, ...
  - Examples: call records, citizen/vehicle/property registrations, ANPR data, passenger records, (filtered) IP-traffic, ...
- **Definition** of bulk: huge volume of personal data, almost exclusively about non-targets
- Bulk collection became visible via Snowden revelations (2013), resulting in changes of law
  - *US freedom act 2015*: no bulk on US persons; non-US persons have rights too (!)
  - *UK Investigative Powers Act 2016*, regime of judicial oversight
  - *NL WiV 2017*, allowing "targeted" bulk interception on cable
- NL oversight turned down bulk interception requestst for many years
  - demonstrates deep disagreeements between services & supervisors
  - core question: what does "targeted" / "focused" bulk mean?

Bulk interception discussion

- Bulk interception only makes sense in combination with automated data analysis (ADA)
- Main points of debate:
  (1) is there a privacy violation if your data are (bulk) intercepted and not selected after data analysis — so not seen by humans?
  (2) for which investigations should bulk + ADA be allowed?
- About (1), difficult!
  - uneasiness remains, because of skewed power relations
  - selection is never perfect, so wrong people may be singled out
  - intelligence services are "black holes", so not much comes out
  - but what about Palantir or Google using similar techniques?
- About (2), relatively uncontroversial goals: (terrorist) threat detection, network defense

Where we are, so far

iCIS | Digital Security
Radboud University

Computer intrusion

- Humint, using (cultivated) spies is slow, risky, and not so reliable
  - e.g. to steal or copy secret documents of opponents
- Hacking is a great alternative
  - It can be done remotely, under the radar, without much risk
  - if succesful, it yields (much) reliable information
  - once inside a position can be re-exploited
- Moreover, hacking at end-points can circumvent encryption
  - at end-points messages exist, necessarily, in unencrypted form
- In the last decades, hacking has become important in intelligence
  - drawback: success is unpredictable, and does not scale
- There are oversight challenges / debates
  - use of unknown vulnerabilities ("zero days", overrated topic)
  - use of commercial tools — like Pegasus of NSO group against Taghi
  - controlling side-damage, to third parties
  - it's unpredictable what will be found — little or much

iCIS | Digital Security
Radboud University

Strategic hacking operations

(1) Planting sleeping malware
  - e.g. in energy, financial, or transport infrastructure
  - nightmare scenario
  - MIVD yearreport 2024: proof of Russians planting malware in NL

(2) Building-up strategic positions
  - e.g. hacking non-target, which access to targets
  - this happened to RSA, to get access to their SecurID tokens
  - is this proportional?

iCIS | Digital Security
Radboud University

Where we are, so far

Concluding remarks

- Power relations, also geopolitically, are determined by access to information flows
- Computer security techniques regulate such access
  - this makes it a socio-political topic
  - basic knowledge of their nature is required to understand the current (and past) world
- Intelligence & security organisations are the most active state organisations in the grey, digital world
  - with both defensive and offensive tasks
  - increasingly visible, assertive role
  - main focus: protection of democtratic order
  - proper regulation is a challenge
  - politisation is a continuous concern

iCIS | Digital Security
Radboud University