Post-Snowden: What does it actually mean? Do we have to change?

Frank Braun

November 14, 2014

what is intelligence (INTEL)?

short: information collection and analysis to guide decision making

classic process:

1. requirements phase: what kind of information is needed?
2. information collection: find good sources and gather info
3. analysis: processing of information
4. goal: guided decision making

why INTEL?

everybody is doing it! it is the most natural thing in the world!

- individual persons
- organizations
  - small companies
  - big corporations
  - intelligence agencies
  - criminal organizations
  - ...

why?

- public-choice theory: people are acting on self-interest
- economics: it's all about efficiency
- game theory: the others are doing it, too!

counterintelligence (CI)

improve:

- physical security
- communications security (COMSEC)
- operations security (OPSEC)

$\Rightarrow$ makes it harder to gather INTEL on you

make it harder to analyze INTEL on you:

- spread misinformation

understand the counter-party better to improve your own process

example: job hunting

requirements:

- what jobs are suitable for my education?
- what kind of salary do I want?

information collection:

- suitable companies in the area
- open positions
- usual salaries

analysis:

- determine good positions / companies
- use the data to plan applications

guided decision making:

- decide on for which positions / companies to apply

counterintelligence:

- clean Facebook page
- up-to-date linked in profile (nice photo, CV)

example: private R&D

requirements:

- what similar projects it the competition working on?
- how can we get ahead of the competition?

information collection:

- open-source intelligence (OSINT)
- how wants to talk about competitor? ex-employees?
- consider even industrial espionage?

analysis:

- get a good overview of the R&D pipeline of competitors

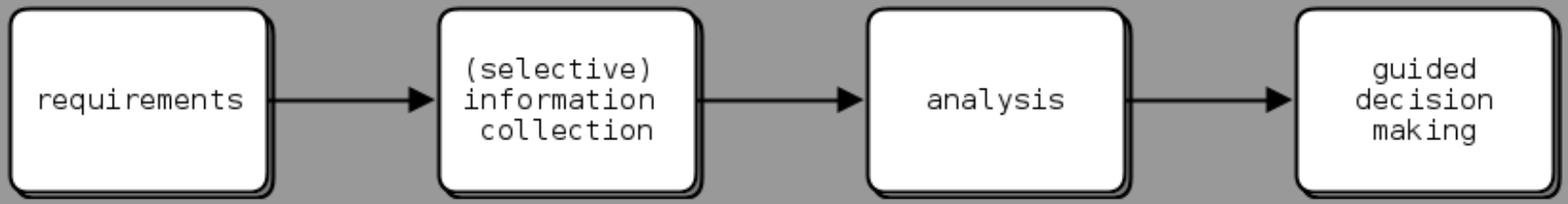
guided decision making:

- what do projects from competitors mean for own R&D?
- prioritize R&D accordingly

counterintelligence:

- keep own projects secret, good OPSEC
- spread misinformation to scare off competitors

old INTEL paradigm



why that order?

- information collection and storage is very expensive

$\Rightarrow$ define requirements first

$\Rightarrow$ gather INTEL only on interesting subjects / topics

example: Stasi (secret police of East Germany)

- 1989: 91,015 employees and 173,081 informants
- one full-time agent for every 166 East Germans
- one of every 63 East Germans collaborated with the Stasi

$\Rightarrow$ greater surveillance than any secret police force in history

$\Rightarrow$ used INTEL for "Zersetzung" (literally: biodegradation)

> *"The goal was to destroy secretly the self-confidence of people, for example by damaging their reputation, by organizing failures in their work, and by destroying their personal relationships. Considering this, East Germany was a very modern dictatorship. The Stasi didn't try to arrest every dissident. It preferred to paralyze them, and it could do so because it had access to* **so much personal information** *and to so many institutions."*

(Hubertus Knabe, German historian)

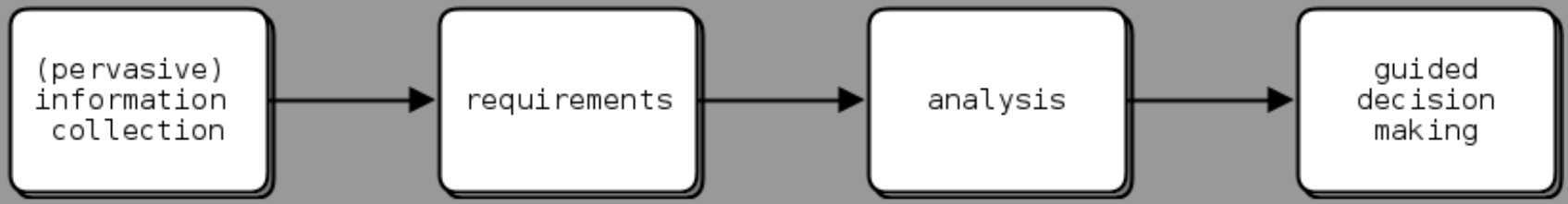
Stasi files

INTEL evolution

information collection and storage ~~is~~ was very expensive:

- a lot of information collection can be completely automated
- requirements phase needs human intervention

$\Rightarrow$ requirements phase (and analysis) dominate costs



old information can be analyzed once a subject becomes interesting

2009: global spying paper (1)

S. Topletz, J. Logan, and K. Williams. Global Spying: Realistic Probabilities in Modern Signals Intelligence. Black Hat USA, 2009.

> *The total cost of surveilling all unique Internet traffic in the world is approximately $4.4b, with a variance of around $500m, depending on what is done with the information. Since the regions of interest are different, with some intelligence organizations focusing on multi-national rather than global surveillance, the cost for non-global mass surveillance of the Internet is less than $1.5b per interested party.*

2009: global spying paper (2)

S. Topletz, J. Logan, and K. Williams. Global Spying: Realistic Probabilities in Modern Signals Intelligence. Black Hat USA, 2009.

> *Although it is not publicly known if any organization does indeed copy and store all unique traffic on the Internet, game theory suggests that if it is both possible and beneficial, then not only is it likely, but also, capable parties will scramble to do so just to remain on par with their counterparts.*

NSA

- budget: classified (estimated $10.8 billion, 2013)
- Utah data center:
  - completed in late 2013 at a cost of $1.5 billion
  - can store data on the order of exabytes or larger. 1 exabyte:

  = 1,000 petabyte
  = 1,000,000 terrabyte
  = 1,000,000,000 gigabyte

total budget for National Intelligence Program (NIP): $45.23b

NSA Utah Data Center

2013: Edward Snowden

NSA's stated objective:

> *"Collect it All," "Process it All," "Exploit it All," "Partner it All," "Sniff it All" and "Know it All."*

(Glenn Greenwald, No Place to Hide)

XKeyScore:

- 2007: 850bn "call events" collected and stored in NSA DB
- $>$ 150bn internet records
- each day: 1-2bn additional records added

http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

2012: the agency was processing $>$ 20bn telecommunications / day

current surveillance

- internet
- mobile phones
- financial information (e.g., credit cards)
- license plate scanners
- flight data

future threats

- cashless society
- widespread face recognition
- Google Glass
- intelligent homes
- Internet of Things

Crypto Wars II

Crypto Wars I: fight against encryption in the 90s, "Clipper Chip" (backdoor), we won
https://www.eff.org/document/crypto-wars-governments-working-undermine-encryption

Crypto Wars II: the fight is back on!

1. war on encryption (default encryption by Apple and Google)
2. war on anonymization (e.g., TOR)
3. war on secure devices (the device backdoor is coming back)

2. & 3. is enough to compromise everybody!

mitigation

- security / privacy is **not** a black-and-white game
- mitigation: make attack more costly than profit

$\Rightarrow$ requires *threat analysis*:

systematic detection, identification, and evaluation of areas or spots of vulnerability of a facility, operation, or system.

- depends on your risk / exposure
- **but:** mass surveillance makes everybody a target!

mitigation technologies

- use cash wherever possible
- free yourself from Facebook
- switch to more secure devices (e.g., Linux laptop)
- use PGP to encrypt emails
- use off-the-record messaging (OTR) for chats
- use mute privacy enhancing communication system[1]
- on Android: use RedPhone for end-to-end encrypted calls
- **better**: get rid of your smartphone altogether!

[1] register for mute news and beta invitation: `http://mute.berlin`

evil and secure devices

- without device control no device security / privacy
- many devices are simply not secure by design
- smartphones contain baseband processors with separate (closed-source) OSs
- backdoors in baseband processors would allow to circumvent main OS[2]

$\Rightarrow$ we need secure (and less complex) devices

[2] claim: https://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor

we have to change

- think about threats and mitigation techniques
- actually use better technology and practice tradecraft

$\Rightarrow$ increase costs for attackers

- there ain't no such thing as a free lunch (TANSTAAFL)
- there ain't no such thing as free privacy (TANSTAFP)

$\Rightarrow$ technology alone won't cut it, we have to change our habits!

key points

1. gathering INTEL is the most natural thing in the world and nowadays a "collect everything" approach is feasible
2. mass surveillance follows from game theory, Edward Snowden's "revelations" weren't actually that surprising
3. to regain our privacy we have to increase the cost of our surveillance drastically (in accordance with threat models)
4. Crypto Wars II: fight over transport encryption is a diversion, the main front is anonymization and device security
5. due to technological trends the threats are getting worse and we are not prepared for it

conclusion

take away:

> *"if we want to regain our personal freedoms and our privacy, we have to change the technologies we use and some of our behavior patterns: there ain't no such thing as free privacy.*

acknowledgments: Jonathan Logan (ideas & discussions)

contacts:

- `frank@cryptogroup.net` (please use PGP, key on key server)
- `94CC ADA6 E814 FFD5 89D0 48D7 35AF 2AC2 CEC0 0E94`
- `#agora` IRC channel / community: `https://anarplex.net/`

register for mute news and beta invitation: `http://mute.berlin`