Attributing Cyber Attacks

Swiss Cyber Storm, 18.10.2017, Lucerne

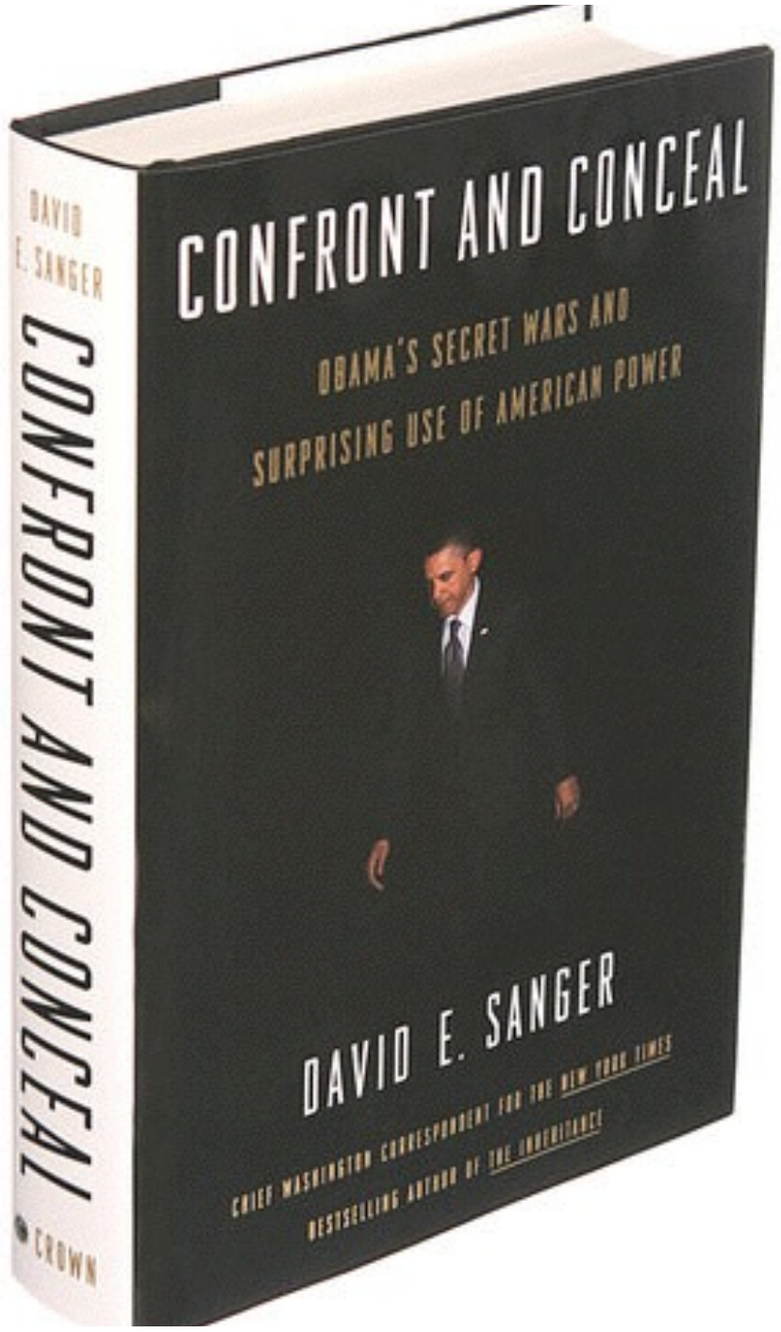
Dr. Clement Guitton

Current assumptions and arguments

Attribution is impossible	vs.	It’s a process
Attribution is technical	vs.	Other elements can be more important
Attribution is cyber attacks is unique	vs.	Not really

First illustrative example

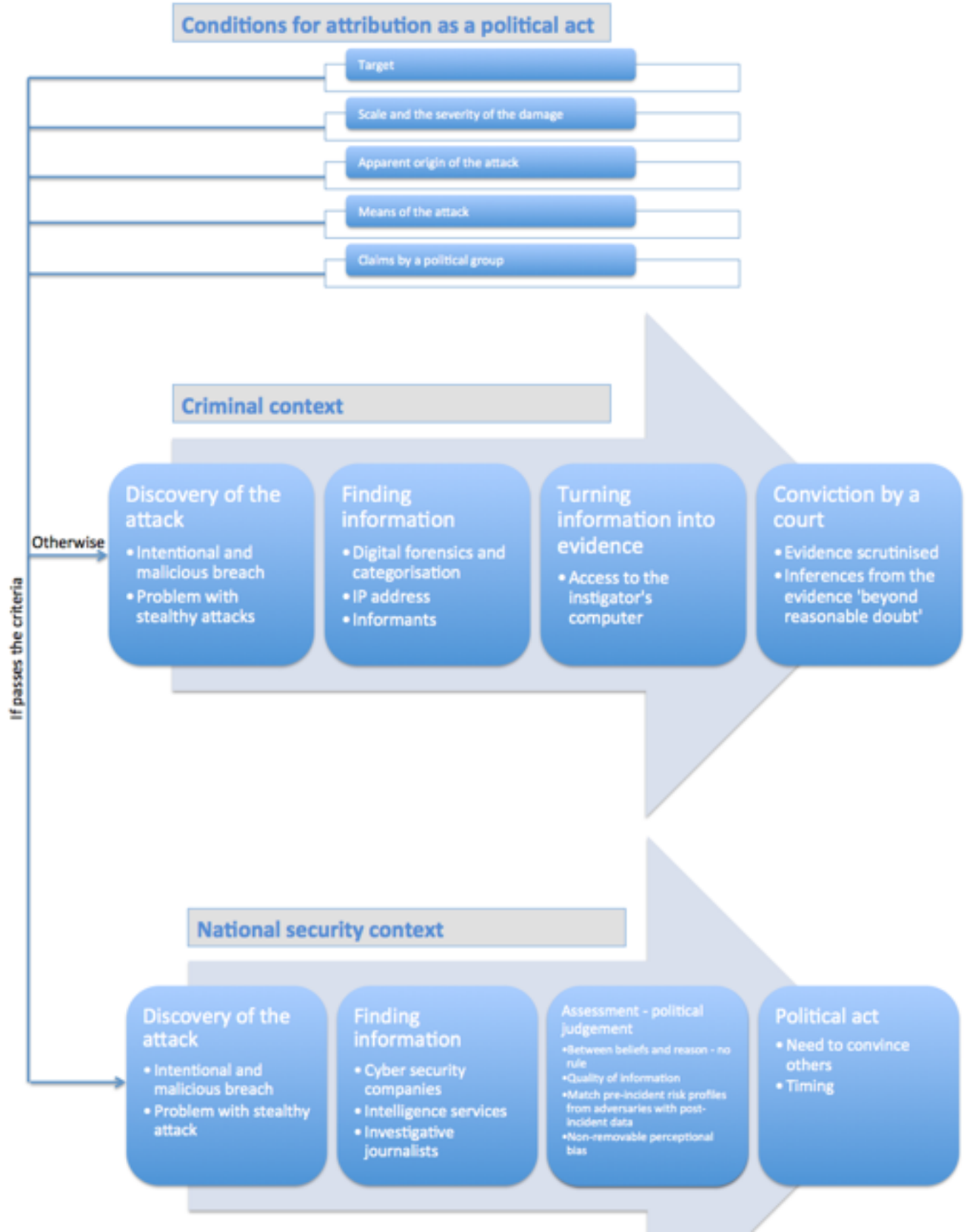
- 2 years time span
- Evidence mainly non-technical
- Journalist work
- Political and need for judgment



Second example

- 2004, Sasser worm
- Millions of computers infected including:
  - Rail system in the UK
  - UK coastguards
  - Italian Interior Ministry
  - European Commission
- Instigator arrested: Sven Jaschan

Two models but same constraints

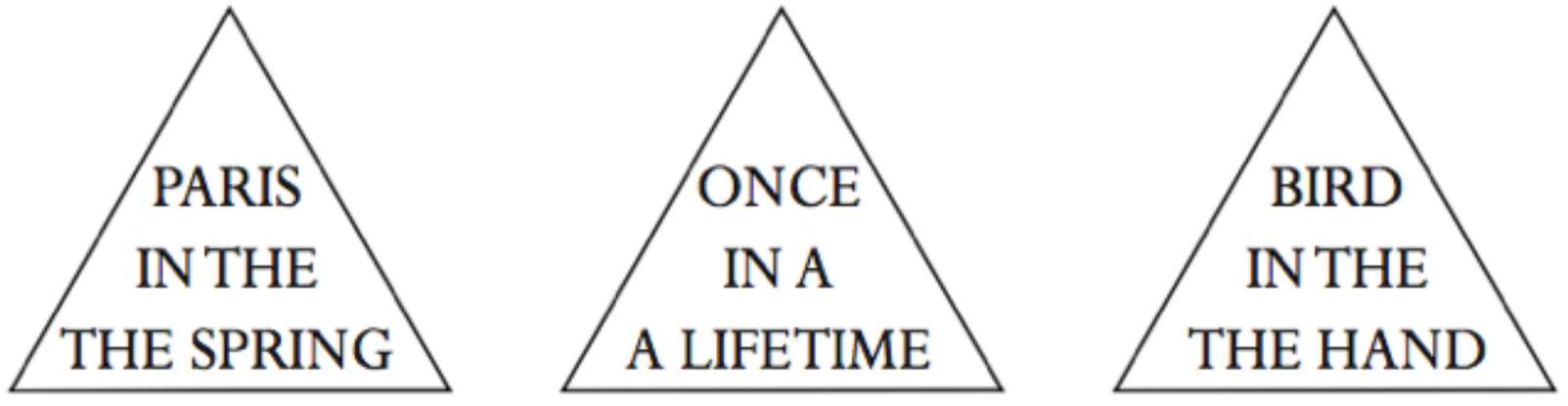


Five Constraints

1. **Reliance on Judgment**
2. Standards of Proof
3. Private Companies
4. Time
5. Plausible Deniability

Constraint 1: Judgment

What can you see?



Foreign Ministry spokesperson: 'making baseless accusations based on premature analysis is irresponsible and unprofessional'

Prof. Lim Chae-ho: 'Future evidence will strengthen the case rather than reverse it'

Reliance on Judgement

Shifts the process from a process focused on collecting and analysing data to a process of convincing a population based on **trust** and **authority**

Two actors matter:

- States: only relevant actors in international system
- Private companies: can re-shape the political agenda

States not immune to ‘groupthink’; companies have conflicting interests

Therefore: attribution always possible to some extent; importance of convincing an audience over gathering evidence

Five Constraints

1. Reliance on Judgment
2. **Standards of Proof**
3. Private Companies
4. Time
5. Plausible Deniability

Constraint 2: Standards of Proof

- Many standards different for individuals, companies, and state — and “beyond reasonable doubt“ very high
- Courts play only a minor role for attribution: verdict binary
- National security context: intelligence more preponderant

State sponsorship: misleading criteria

Circumventing frustration with circumstantial and non-conclusive evidence

Geopolitical context
Apparent origin of the attacker
Political character of the victim
Sophistication
Scale of the attack
Beneficiaries

Five Constraints

1. Reliance on Judgment
2. Standards of Proof
3. **Private Companies**
4. Time
5. Plausible Deniability

Constraint 3: Private Companies
Three arguments used to undermine them

Rise of the cybermen

Name	From	To	Date joined private sector
Sameer Bhalotra	Senior director for cyber-security, White House	COO of Impermium	Aug 2012
Steve Chabinsky	Deputy assistant director, cyber division, FBI	Senior vice-president of legal affairs and chief risk officer, CrowdStrike	Sep 2012
Shawn Henry	Executive assistant director, FBI	President of CrowdStrike Services	Mar 2012
Sean McGurk	Director, Department of Homeland Security control-system security programme	Chief policy officer at ICS Cybersecurity, then at Verizon	Sep 2011
Scott O'Neal	Deputy assistant director of cybercrime, FBI	Consultant at Booz Allen Hamilton, then director at Mandiant	Aug 2009
Howard Schmidt	Co-ordinator for cyber-security, White House	Board of directors at Qualys, then founder of Ridge Schmidt Cyber	Jun 2012
Mark Weatherford	Deputy undersecretary for cyber-security, Department of Homeland Security	Principal, the Chertoff Group	May 2013

Source: *The Economist*

KASPERSKY lab

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

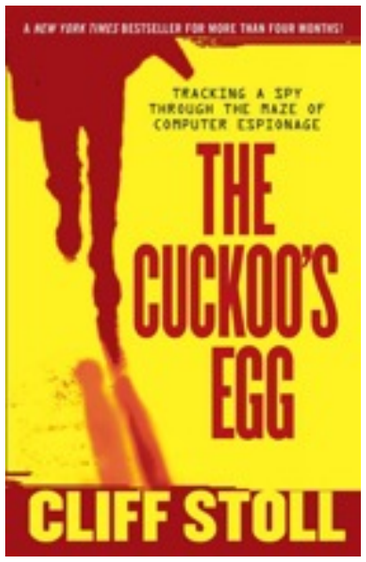
MANDIANT

Five Constraints

1. Reliance on Judgment
2. Standards of Proof
3. Private Companies
4. **Time**
5. Plausible Deniability

Constraint 4: Time

- Attribution: ‘the lack of certainty sufficient [to classify the incident] as a *casus belli* in real time, and by technical means alone’



- Historically, reduction of time in attribution via improvement of judicial procedures rather than through technical innovation

- Value for ‘real time attribution’?
  Criminal context: DDoS, deterrence (celerity), intellectual property
  Nat. sec: impossible, empirical evidence against it, dismisses context (also relevant for criminal attacks)

Five Constraints

1. Reliance on Judgment
2. Standards of Proof
3. Private Companies
4. Time
5. **Plausible Deniability**

Plausible deniability

- Relies on bureaucratic “trickeries“
- Counter-intuitive: use groups with closer ties to government

- Who is it directed to?
  - Secrecy: the bureaucracy argument & shielding officials from prosecution
  - Controversial? Morally difficult to justify cyber attack at home?
  - Military signals are notoriously ambiguous
    - Sabotage and espionage operations abroad, unclear: accepted but coercion requires clarity; but avoiding retaliation important too (strategic ambiguity, “over covert op“)
    - Strong deniability for sabotage at home – although not as polemical anymore as not so violent
    - Strong deniability for espionage at home

Conclusion

- Attribution is possible, non-technical, and non-unique

- Two policy lessons: collection and interpretation
  - Focus on meta-data recently: a lot more is possible and less privacy intrusive for attribution
  - Use strict framework like Analysis of Competing Hypotheses to minimise biases; clearly show thought-process

Thank you!

(free copies available)