Breaching the Bundestag: A Preliminary Case Study of the Policy Response to the Spring 2015 Cybersecurity Incident at the German Parliament

Christine Pommerening, Ph.D.

George Mason University

9th Annual Homeland Defense and Security Education Summit

Orlando, FL - September 25, 2015

Getty images

OVERVIEW

1. The Case Study Method
2. The Context
3. The Incident
4. The Response
5. The Case Study Setup
6. References

1. THE CASE STUDY METHOD

Concept

Qualitative Research Method

Detailed examination of a single (or few) instance(s) of a class of phenomena

Design Components

1. Selecting the research question(s)
2. Defining the proposition(s)
3. Defining the unit(s) of analysis
4. Linking the data to propositions
5. Interpreting the findings
6. Reporting the results

1. THE CASE STUDY METHOD

1. Selecting the Research Question(s)

(a) Focus of the study is to answer "how" and "why" questions;

(b) Behavior of those involved in the study cannot be influenced;

(c) Examination of contextual conditions relevant to the phenomenon

(d) Boundaries are not clear between the phenomenon and context

2. Defining the Proposition(s)

(a) Explanatory: presumed causal links in real-life interventions

(b) Exploratory: intervention being evaluated has no clear, single set of outcomes

(c) Descriptive: intervention or phenomenon and the real-life context in which it occurred

(d) Single: unique/extreme/critical cases

(e) Multiple: routine cases, to predict similar or contrasting results

1. THE CASE STUDY METHOD

3. Defining the Case

1. Unit of Analysis

(a) Individual

(b) Program

(c) Process

(d) Organization

(e) Differences

2. Boundaries

(a) By time and place

(b) By time and activity

(c) By definition and context

1. THE CASE STUDY METHOD

4. Analysis

1. Techniques

(a) Pattern-matching

(b) Explanation-building

(c) Time-series analysis

(d) Logic models

(e) Cross-case synthesis

2. Concerns

(a) Validity

(b) Concurrency

1. THE CASE STUDY METHOD

5. Interpretation

1. Framework
2. Findings
3. Recommendations

1. THE CASE STUDY METHOD

6. Reporting

(a) Linear

(b) Comparative

(c) Chronological

(d) Theory-building

(e) Suspense-building

(f) Unsequenced

1. THE CASE STUDY METHOD

Case Method of Teaching

Presentation of (actual or fictionalized) events to establish a framework for discussion

Commonality

Focus on decision-making: why taken, how implemented, what result, which alternatives

3. THE CONTEXT

1. Bundestag

- Federal Parliament
- Proportional representation, with thresholds and direct elections
- Governing coalition
    - Christian Democratic Union (CDU): 255
    - Christian Social Union (CSU): 56
    - Social Democratic Party (SPD): 193
- Opposition parties
    - The Left (DIE LINKE): 64
    - Alliance '90/The Greens (Die Grünen): 63
- Leadership
    - 1 President: Norbert Lammert, SPD
    - 6 Vice Presidents: One from each party represented

2. THE CONTEXT

2. Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Federal Office for Information Security (est. 1991)
- Central cybersecurity agency within and for the federal government
- Administrative Oversight: Federal Ministry of the Interior
- Tasks: Threat Assessment and Risk Information, Breach Investigation, and Solutions Development
- Operational Units: CERT-Bund, IT-Lagezentrum, Cyber-AZ
- Similar U.S. agencies: NIST, NPPD

3. Bundesamt für Verfassungsschutz (BfV)

- Federal Office for the Protection of the Constitution (est. 1950)
- Tasks: Collection and analysis of information on man-made threats
- Similar U.S. agencies: FBI, NSA

2. THE CONTEXT

Background

- 3,500 probes (avg/day) on malware servers
- 1,100 website operators notified of malware distribution
- 34 systems (year) infected with malware
- 20 attacks (avg/day) on government networks not recognized through standard protective measures (commercial anti-virus software and firewalls)
- 1 targeted attack (avg/day) suggests a sophisticated intelligence background
- 1 DoS attack (avg/month) on federal websites
- Foreign Affairs, Defense, Security, Finance
- Increase in attacks around high-profile events

Source: BSI (2015) Die Lage der IT-Sicherheit in Deutschland 2014, p.28ff.

3. THE INCIDENT

Incident Response

08 May: Bundestag IT Dept notices unusual amount of data on server connected to a Rep PC

12 May: BfV warns Bundestag of possible targeted cyberattack (not released at the time)

15 May: Faction IT Depts inform Representatives and staff of "security incident"

15 May: Partial shutdown and reboot of Parlakom intranet

15 May: Initial media reports of a cyberattack on the Bundestag (Der Spiegel)

15 May: BSI confirms "assisting Bundestag in incident analysis" (Press release)

15 May: Petra Pau, Bundestag vice president and IT Committee (IuK) chair, confirms breach

16 May: Norbert Lammert, Bundestag president and chief of administration, leads response

16 May: Numerous media reports, citing anything from DDoS to corrupt hardware

19 May: Lammert adds private BFK EDV-Consulting to assist BSI

11 June: Lammert announces inclusion of BfV in investigation, but w/o access to Parlakom

22 June: Bundestag decides to use summer recess to reinstall software, exchange pw server

21 Aug: Entire Parlakom system (20,000nodes) taken offline and rebooted (through 24 Aug)

Trojan distributed via email (reportedly from a spoofed un.org domain) that linked to an infected website, found on 15 of the 20,000 Parlakom computers

4. THE RESPONSE

Administrative Response

Bundestag has contracted with private corp. T-Systems, to be assisted by BSI, to

- Analyze the entire IT-Infrastructure for vulnerabilities
- Conceptualize a new system
- Reconfigure the new system

First steps include

- Blocking 10,000 websites
- Administration of the blocked list through BSI
- Oversight through IuK Commission
- Possibly restriction on use of memory sticks and smartphones
- Increased IT staff and training

4. THE RESPONSE

Political Response

"Debakel sondergleichen" [Unique debacle] *Fmr. Minister of Interior, Otto Schily*

"Beachtlich" [Remarkable] *BfV President Dr. Hans-Georg Maaßen*

"Peinlich" [Embarrassing] *Spokesperson of Chaos Computer Club, Constanze Kurz*

"Völlig unzureichend" [Totally lacking; re information sharing by the Bundestag president] *Spokesperson of Die Grünen [Green], Konstantin von Notz*

"Kaum Kommunikation und große Verunsicherung" [hardly any communication and high insecurity; re information sharing by Bundestag president] *Rep. Lars Klingbeil of the SPD [Social Democrats*]

"Das Haus brennt" [The house is on fire; re resistance of opposition to BfV and BSI] *Rep. Armin Schuster of the CDU [Conservatives]*

"Ein Wettlauf der Geheimdienste schafft nicht mehr Sicherheit" [Intelligence agencies' arms race does not increase security; re involvement of BSI and BfV] *IuK chair Petra Pau of Die Linke [The Left]*

"Open-Source als Lösung" [Open-Source solutions; re revamping of system] *Spokesperson of Die Linke [The Left], Ulla Jelpke*

4. THE RESPONSE

Policy Response

1. IuK Committee hearings

- Closed session on 21 May
- Preliminary internal investigation report
- Protocol published on 11 June by tabloid [BILD]

2. Council of Elders

- Compromise agreement on scale and scope of external assistance

4. THE RESPONSE

Policy Response

3. IT-Sicherheitgesetz [IT Security Act], passed by parliament 10 June, effective 25 July 15

Original scope, put forth by cabinet on 17 Dec 14, obligates CI owners and operators to:

- Maintain minimum level of IT-security
- Provide proof of maintenance through security audits
- Report significant security incidents to the BSI
    - Estimated 2,000 companies affected
    - Estimated 7 reports per company per year
- Establish a process and point of contact
- Increased obligations for ICT providers to warn customers of misuse of their equipment
- BSI allowed to test, evaluate, and publish findings on commercial IT products

Final amendment, introduced post-breach by coalition factions:

- Federal agencies and Bundestag to be subject to same rules as CI owners

5. THE CASE STUDY SETUP

1. Selecting the Research Question(s)

(a) Focus of the study is to answer "how" and "why" questions;
→ How was the technical and administrative response to the Bundestag breach influenced by political factors?

(b) Behavior of those involved in the study cannot be influenced;
→ Ex-post observation

(c) Examination of contextual conditions relevant to the phenomenon
Context of federal government affecting cybersecurity response

(d) Boundaries are not clear between the phenomenon and context

2. Defining the Proposition(s)

(a) Explanatory: presumed causal links in real-life interventions

(b) Exploratory: intervention being evaluated has no clear, single set of outcomes

(c) Descriptive: intervention or phenomenon in its real-life context

(1) Single: unique/extreme/critical cases

(2) Multiple: routine cases, to predict similar or contrasting results

5. THE CASE STUDY SETUP

3. Defining the Case

1. Unit of Analysis

(a) Individual

(b) Program

(c) Process

(d) Organization: Bundestag

(e) Differences

2. Boundaries

(a) By time and place

(b) By time and activity

(c) By definition and context: Cybersecurity incidents in federal government

5. THE CASE STUDY SETUP

4. Analysis

1. Techniques

(a) Pattern-matching

(b) Explanation-building:
Establishing timelines, progressions, correlations for incident and response

(c) Time-series analysis

(d) Logic models

(e) Cross-case synthesis

2. Concerns

(a) Validity

(b) Concurrency of collection and analysis: Post-incident only

5. THE CASE STUDY SETUP

5. Interpretation

1. Framework: Multiple Streams Approach of the Policy Process

    1. Problem Stream

        Indicators: data, reports, budgets

        Focusing Events: disasters, experiences, symbols

        Feedback : surveys, elections, published opinions

    2. Policy Stream

        Actors: Administrators, Staffers, Interest Groups, Individuals ("policy entrepreneurs")

        Alternatives: research and ideas

    3. Politics Stream

        Actors: Appointees, Congress, Media, Interest Groups, Elites

        Agenda-setting, Consensus-building, Legislating

    → Convergence of streams; windows of opportunity

5. THE CASE STUDY SETUP

5. Interpretation

2. Interpretation:

1. Problem Stream

Indicators: 2015 BSI Report

Focusing Event: May 2015 cyberattack

Feedback

2. Policy Stream

Actors: Bundestag president, BSI, BfV, IT security community

Alternatives: IT-Security Act amendments

3. Politics Stream

Actors: Representatives and Committees, media investigation and leaks

Agenda-setting, Consensus-building, Legislating: IT-Security Act Passage

→ Convergence of streams; windows of opportunity

5. THE CASE STUDY SETUP

6. Reporting

(a) Linear

(b) Comparative

(c) Chronological

(d) Theory-building

(e) Suspense-building

(f) Unsequenced

6.REFERENCES

Bewarder, Manuel, *Verfassungsschutz verfolgt Spur nach Russland,* Die Welt, 11 June 2015. Available at http://www.welt.de/politik/deutschland/article142372328/Verfassungsschutz-verfolgt-Spur-nach-Russland.html Accessed 24 Sept 2015 Accessed 24 Sept 2015.

Bundesamt für Sicherheit in der Informationstechnik (BSI), *Die Lage der IT-Sicherheit in Deutschland 2014*, Bonn: BMI, 2015.

Kingdon, John W., *Agendas, Alternatives, and Public Policies*, Boston: Little, Brown, I984.

Kommission des Altestenrates für den Einsatz neuer Informations- und Kommunikationstechniken und-medien (IuK), *Protokoll der 6. Sitzung vom 21. May 2015,* Berlin: Bundestag, 2015.

Obermayer, Bastian, *Bundestag bekommt Hackerangriff nicht unter Kontrolle,* Süddeutsche Zeitung, 10 June 2015. Available at http://www.sueddeutsche.de/politik/berlin-bundestag-bekommt-hackerangriff-nicht-unter-kontrolle-1.2515345 Accessed 24 Sept 2015.

Potsdamer Konferenz für Nationale CyberSicherheit, Hasso-Plattner-Institut, Potsdam, 11- 12 June 2015. https://www.potsdamer-sicherheitskonferenz.de

Yin, Robert K., *Case Study Research: Design and Methods, 3rd Edition* (Applied Social Research Methods, Vol. 5), Thousand Oaks, CA, Sage. 2003.

Cyber-Incident Information Sharing Framework in the EU