BfV Bundesamt für Verfassungsschutz



# Digitale Wirtschaftsspionage – Deutsche Wirtschaft im Fokus fremder Nachrichtendienste

# Aktuelle Herausforderungen

# Zuständigkeiten der Cyberabwehr

**kriminelle Akteure:**

- Ransomware
- DDoS-Angriffe
- Defacements

**Staatliche / extremistische Akteure:**

- APT-Kampagnen
- DDoS-Angriffe
- False-Flag Operationen
- weitere

# Aufgaben des BfV

- **Prävention**
  - Indicators of Compromise (Cyber-Brief)
  - Sensibilisierungen
  - Gefährdungsanalysen
- **Detektion**
  - Server-Überwachung nach G10
  - HUMINT
  - Technische Analyse
- **Attribution**
  - Aufklärungsinteresse
  - Opferfläche
  - Fähigkeiten des Angreifers

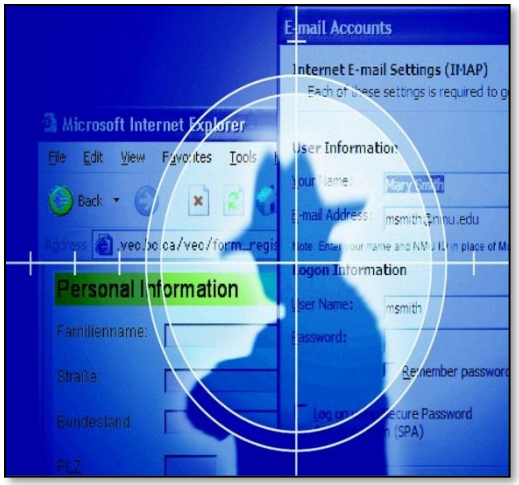
Bundesamt für
Verfassungsschutz

# Cyberbedrohungen

# Aufklärungsinteresse fremder Nachrichtendienste

- Politik:
  - Außenpolitik
  - EU-Erweiterungspolitik
  - Supranationale Organisationen

- Institutionen:
  - Think-Tanks
  - Institutionen im Umfeld des G20 / T20-Gipfels
  - Oppositionen / Dissidenten



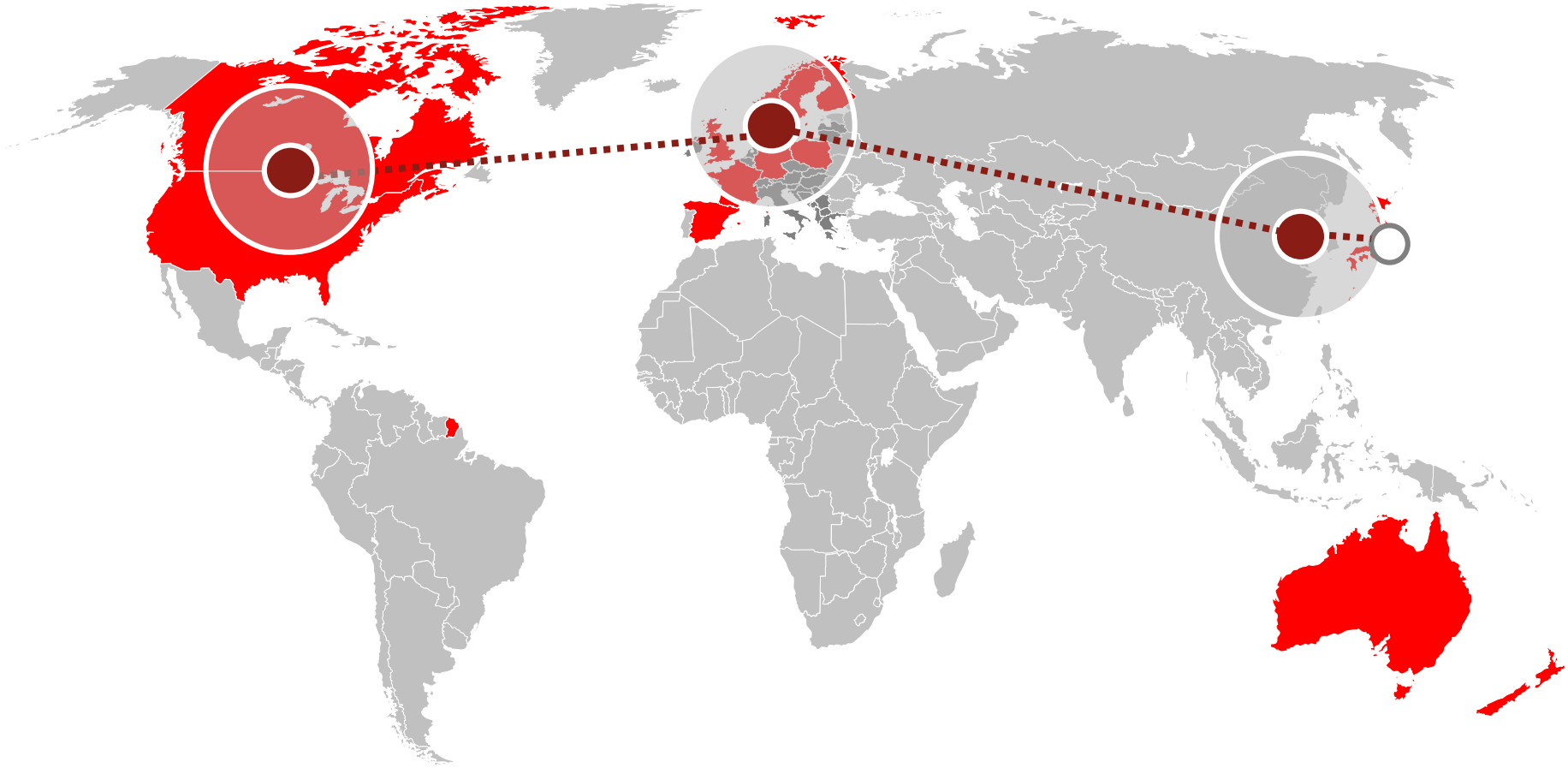

- Wirtschaft:
  - Energiewirtschaft
  - Healthcare / Chemie
  - Luft- und Raumfahrt
  - sonstige Hochtechnologien
  - B20-Gipfel

# Gründe für Cyberangriffe

- **Eigenschaften**
  - **geringer personeller / finanzieller Aufwand** im Vergleich zur „klassischen“ **Spionage**
  - universell einsetzbar
  - auch für **Sabotagezwecke**
  - **zeitlich** steuerbar


- **Fünf Minuten** für Manipulation einer E-Mail-Anschrift
- **Schadsoftware** über Anhang von **E-Mails** oder **Link** auf kompromittierte Webseiten
- **Geringes Risiko** für den Angreifer (entdeckt zu werden)
- Und wenn doch – **welche Konsequenzen** hat es?

# Initiierung - Zielauswahl

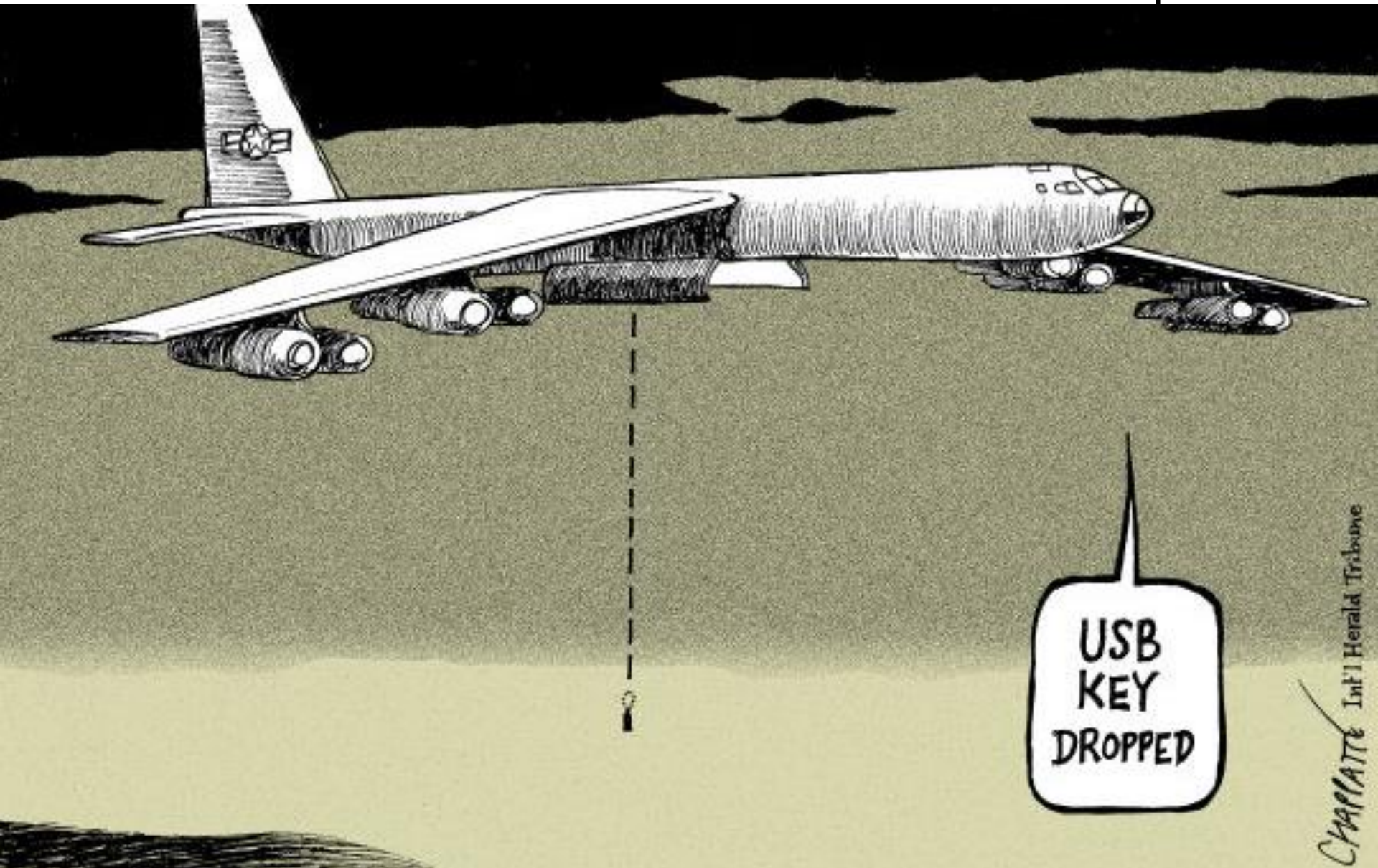


# Initiierung - Aufklärung

- **Jobbörsen**
  - Können Aufschluss über eingesetzte Technik geben
- **Soziale Netzwerke**
  - Preisgabe von internem Wissen
  - Fake-Profile
- Teilweise Verlust über **Datenhoheit**

⇨ Social Engineering

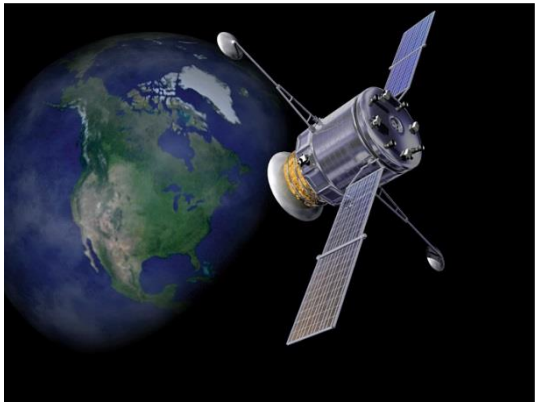
# Modus Operandi



# Hybride Kriegsführung?

- Land
- See
- Luft
- Weltraum
- **Cyberspace**

Von Spionage bis zu Sabotage!

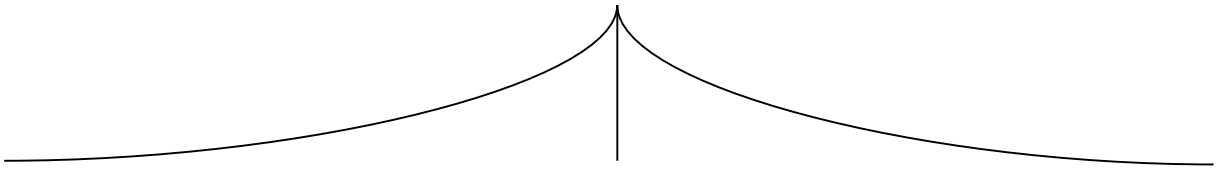



# Durchführung

- Zusammenstellung der Angriffswerkzeuge
- Auswahl der Angriffspunkte:
  - Spear-Phishing
  - Watering-Hole
  - Soziale Netzwerke

# Während eines DDoS-Angriffes…

…stellen **74%** der Unternehmen einen weiteren Sicherheitsvorfall fest!



**43%**
**Malware**

**32%**
**Hacking / Network Intrusion**

**25%**
**Datenleak**

Das Ziel eines Cyberangriffes ist nicht immer direkt ersichtlich **!**

Quelle: IT Security Risks Survey 2015, Kaspersky Lab

# Modus Operandi: Sabotage von SCADA-Systemen

Cyber-Sicherheit

## Die Hackerdämmerung

**Ein Stromausfall in der Ukraine könnte durch einen Cyber-Angriff ausgelöst worden sein. Es wäre das erste Mal, dass ein Stromnetz über das Internet lahmgelegt wurde.**

11.01.2016, von PIOTR HELLER



© ILLUSTRATION F.A.S./FOTO KRZYSZTOF LASO

Auch der stärkste Strom steht still, wenn „Black Energy" es will.

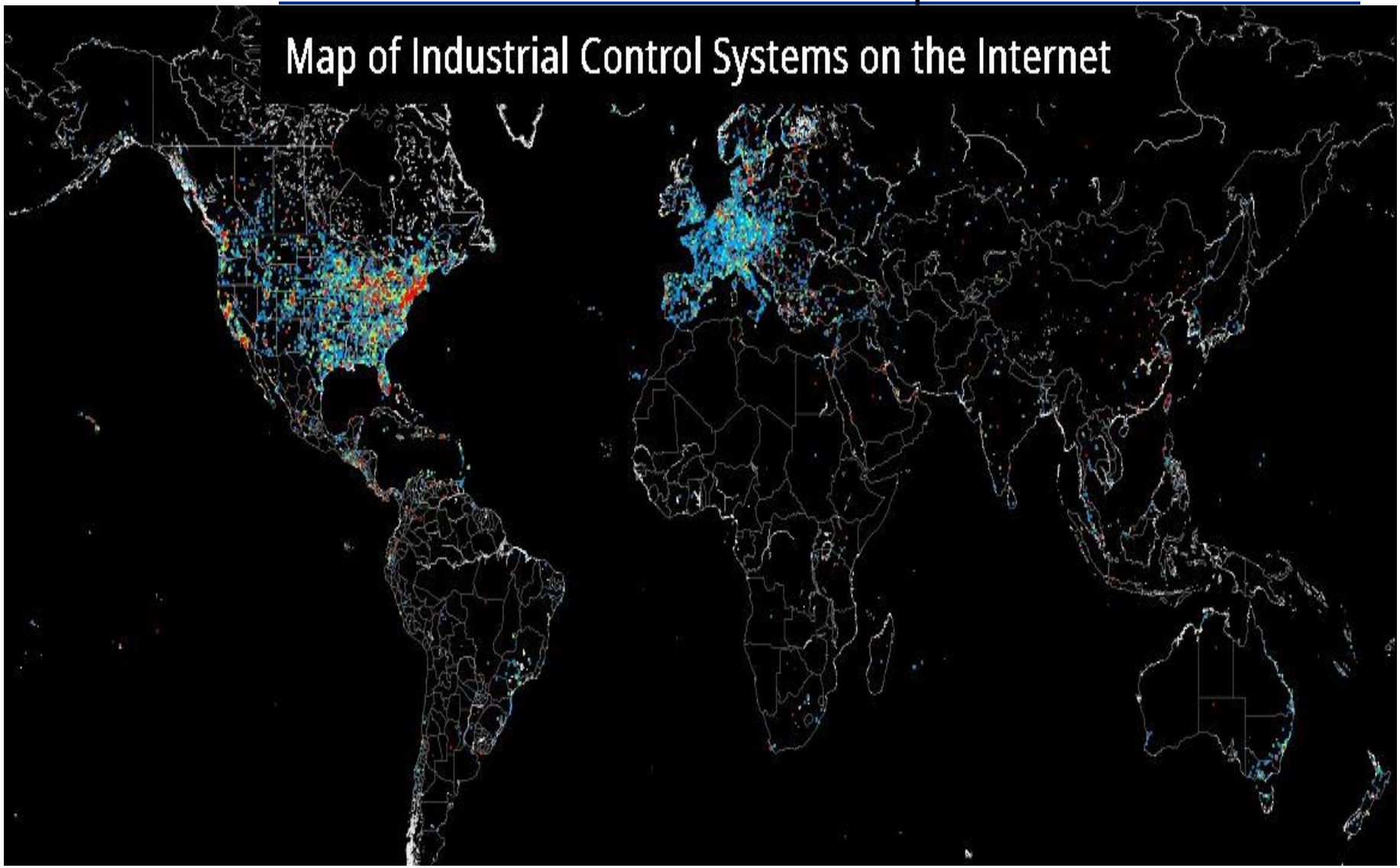
## Ukraine: Hackerangriff verursachte Blackout

Florian Rötzer 07.01.2016

Nach IT-Sicherheitsfirmen könnte es sich um den ersten Fall handeln, bei dem ein Stromnetz durch einen Hackerangriff lahmgelegt wurde

Offenbar haben es Hacker geschafft, einen Stromausfall zu verursachen. Am 23. Dezember war in einem großen Teil des Oblasts Ivano-Frankivsk mitsamt der Hauptstadt in der Westukraine für mehrere Stunden der Strom ausgefallen. Nach einem lokalen Medium, das am 24. darüber berichtete, sei dafür ein Computervirus verantwortlich gewesen. Hacker seien danach in das Steuerungssystem des Energiekonzerns Prykarpattyaoblenergo eingedrungen.

# SCADA: Der Schwachpunkt des Westens?



Shodan | Developers | Book | View All...

SHODAN | scada | Explore | Enterprise Access | Contact Us

Exploits | Maps

## TOP COUNTRIES

| | |
|---|---|
| Canada | 78 |
| United States | 74 |
| Bulgaria | 55 |
| Spain | 13 |
| Serbia | 11 |

## TOP SERVICES

| | |
|---|---|
| FTP | 92 |
| HTTP | 73 |
| SNMP | 32 |
| NetBIOS | 30 |
| Modbus | 21 |

## TOP ORGANIZATIONS

| | |
|---|---|
| Telus Communications | 34 |
| Telus Mobility | 30 |
| Verizon Wireless | 25 |
| Terra S.p.a. | 7 |
| Com4 AS | 7 |

## TOP OPERATING SYSTEMS

Total results: 322

**213.208.49.244**
Onlime GmbH
Added on 2016-02-25 05:39:23 GMT
Germany
Details

```
nServerName;SCADA;InstanceName;SA;IsClustered;No;Version;8.00.194
tcp;3259;np;\\SCADA\pipe\MSSQL$SA\sql\query;
```

**185.16.166.228**
Athens International Airport SA
Added on 2016-02-23 17:27:39 GMT
Greece, Athens
Details

```
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Error returning browse list: NT_STATUS_ACCESS_DENIED
Anonymous login successful

        Server               Comment
        ---------            -------
        SCADA
```

**50.77.64.129**
50-77-64-129-static.hfc.comcastbusiness.net
Comcast Business Communications
Added on 2016-02-23 19:41:27 GMT
United States, Jersey City
Details

```
{ServerName;SCADA-MAIN;InstanceName;SQLEXPRESS;IsClustered;No;Ver
```

**173.182.108.83**
Telus Communications
Added on 2016-02-23 19:16:44 GMT
Canada
Details

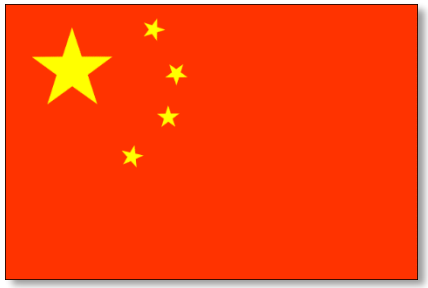
```
220 Teepee SCADA (00:0F:92:00:7F:75) FTP server ready.
550 Can't set guest privileges.
214- The following commands are recognized (* =>'s unimplemented).
   USER    PORT    STOR    MSAM*   RNTO    NLST    MKD     CDUP
   PASS    PASV    APPE    MRSQ*   ABOR    SITE    XMKD    XCUP
```

Bundesamt für
Verfassungsschutz

# Maßnahmen

# Analyse

## Indizien für Steuerung durch fremde ND:



- Modus Operandi
  - Angriffsvektor
  - Malware
  - Rückmeldewege
  - Server-Infrastruktur
  - 0-Day-Exploits
  - Einsatz von Botnetzen
- Attribution
  - Opferfläche
  - Aufklärungsinteresse
  - Überschneidungen zu anderen Kampagnen

# Maßnahmen des BfV

- **Informationsweitergabe**
  - Bei einer möglichen Betroffenheit
  - Nach einer Kontaktaufnahme
  - Zur Identifikation des Angreifers
  - Zum Hintergrund des Angriffes

- Beobachtung und Analyse von Cyberangriffen im **internationalen Verbund**


- **Informationssharing** (anonym!)

# Partner der Wirtschaft und Politik


- Hausinterne Publikation, seit Oktober 2015
- Verteilung an Interessenten aus Wirtschaft, Wissenschaft, Politik und Verwaltung
- Übermittlung konkreter Indizien einer aktuellen Cyberangriffskampagne

BfV
Bundesamt
für Verfassungsschutz



**Vielen Dank für Ihre Aufmerksamkeit!**

**Haben Sie noch Fragen?**