Technische Hochschule
Brandenburg
University of
Applied Sciences

KI auf Angreifer- und auf Verteidigerseite: **Wer hat die Nase vorne?**

Ivo Keller* und Dragoljub Milasinovic
*Studiengangsdekan *Security Management (M.Sc.)*
TH Brandenburg
keller@th-brandenburg.de, +49 3381 355-278

Security Management (M. Sc.)

Prof. Dr. Ivo Keller

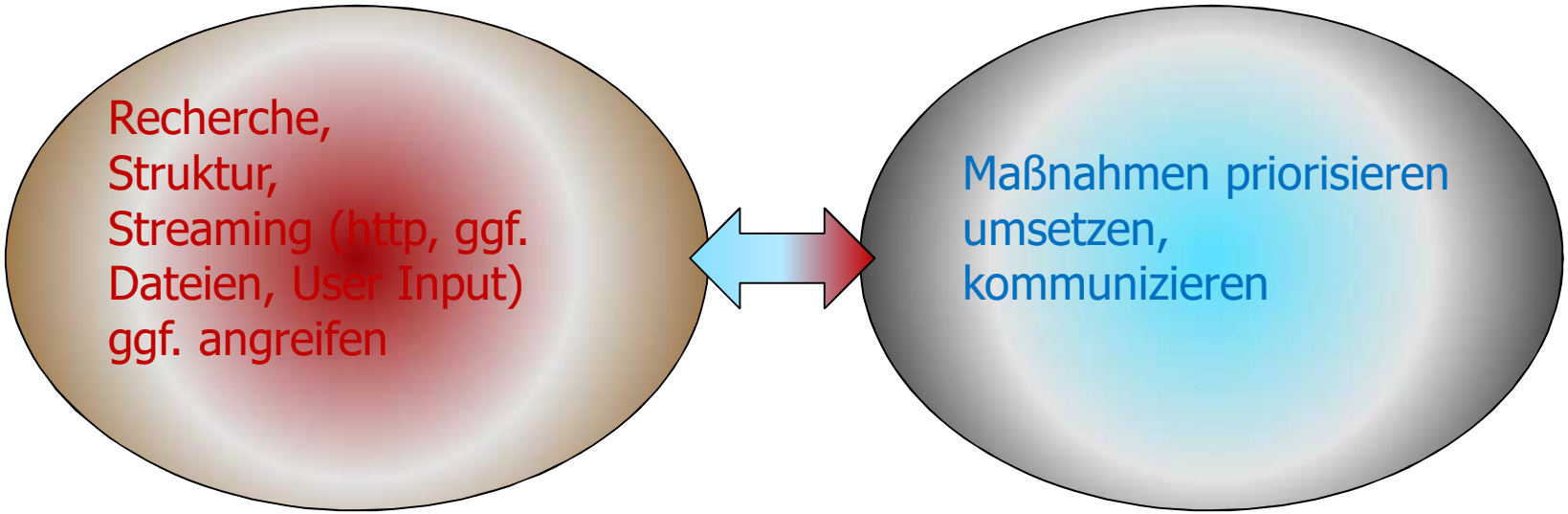
- Koordination der Dozenten
  - Secure SDL, Pentest, Secure Data Center, Cyberwar
  - Social Engineering, Business Continuity, ISMS, KRITIS
- *Secure Systems Lifecyle Management, Process Mining, Predictive Business*

Dragoljub Milasinovic, B.Sc. Inf.

- *Data Science, Maschinelles Lernen, Web Computing*

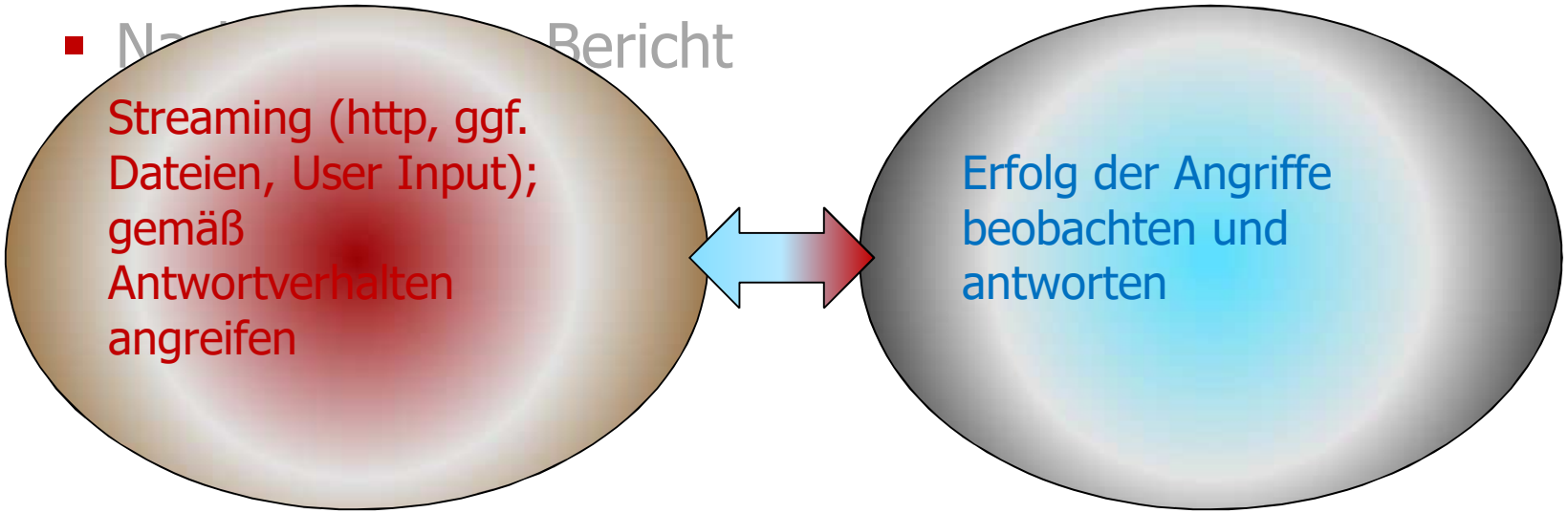
Angreifer und Verteidiger

- Härten durch Pentest
  - juristische Vorbereitung (Whitebox)
  - Vulnerability Scan, Exploitation
  - Nachbereitung
  - Bericht



Angreifer und Verteidiger

- Härten durch Fuzzy Pentest
  - juristische Vorbereitung (Whitebox)
  - Vulnerability Scan, Exploitation
    - Muster-Katalog (welche Kategorie erfolgreich?)
    - Sequenzen (Exploits)
  - Na[illegible] Bericht

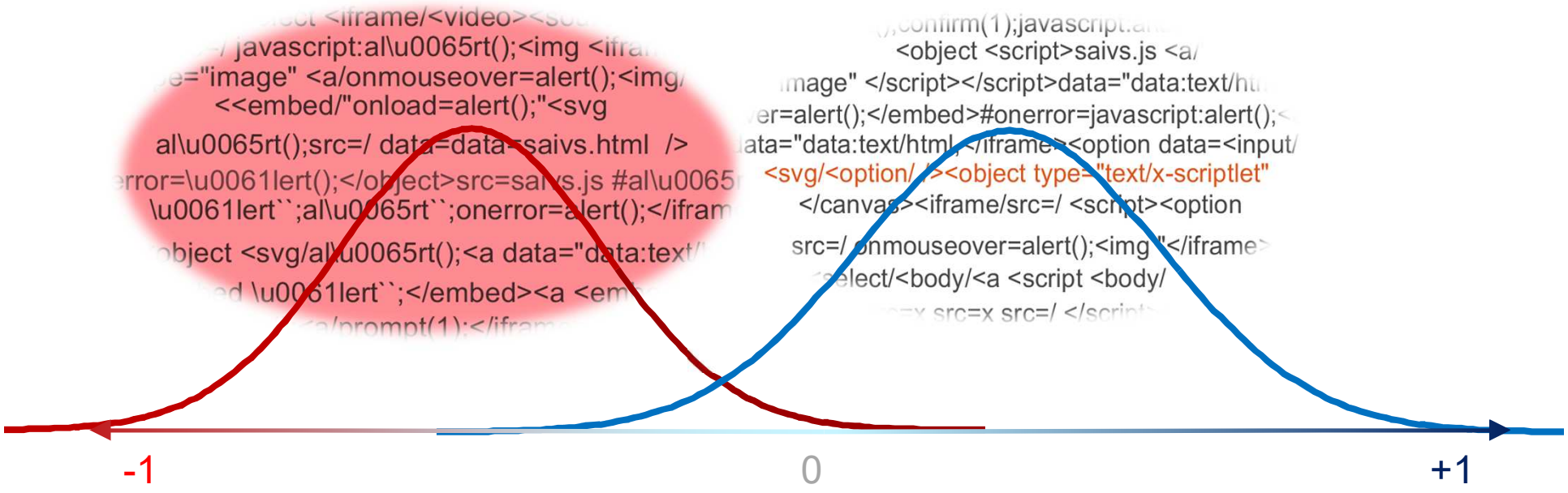


Wenn ich aber nur 3 Beispiele habe?

- Synthetisch: Angriffsmuster und Harmloses
  - Vorgabe von bekannten Mustern,
  - da

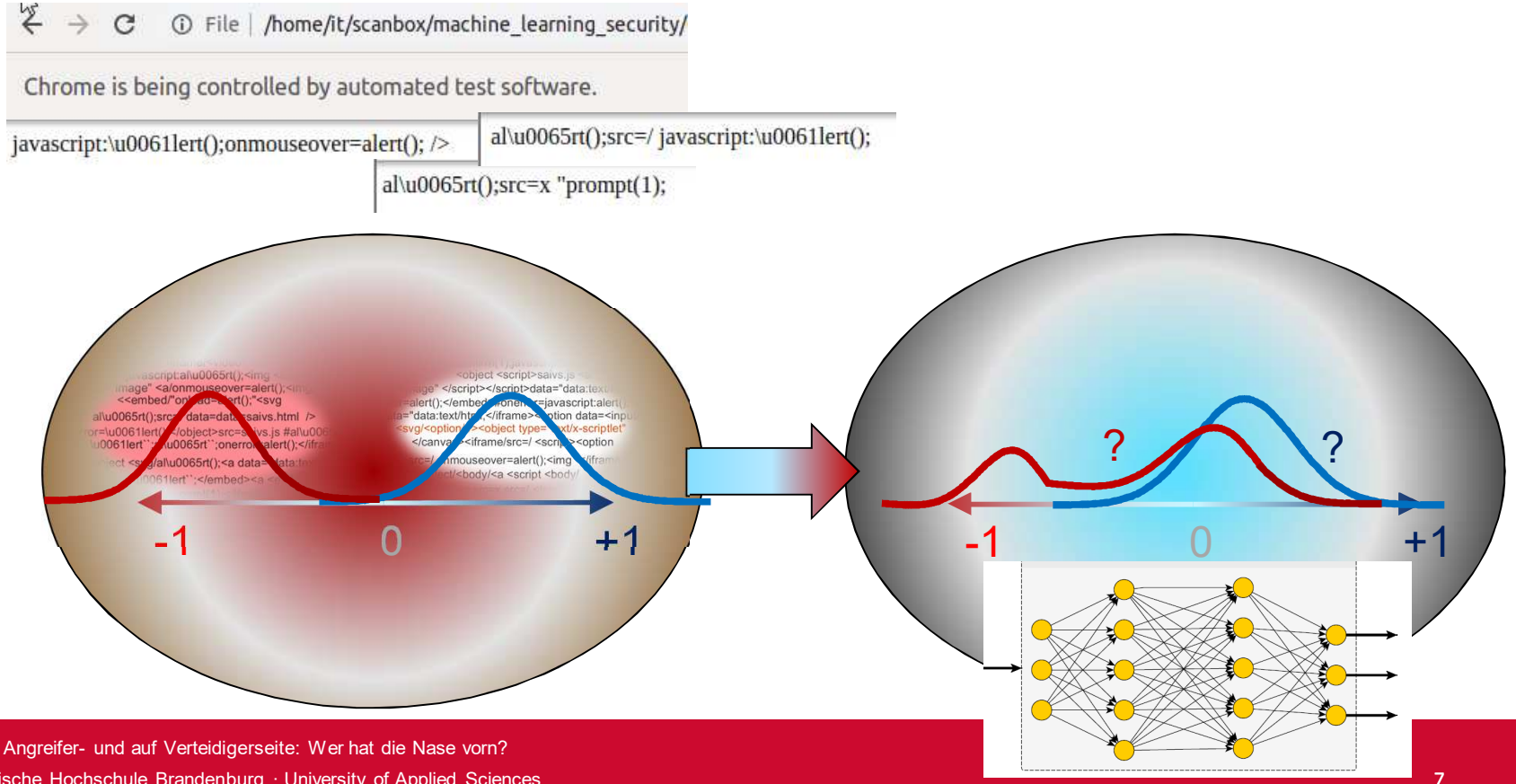
Wenn ich aber nur 3 Beispiele habe?

- Synthetisch: Angriffsmuster und Harmloses
  - Vorgabe von bekannten Mustern,
  - dann Variationen erzeugen



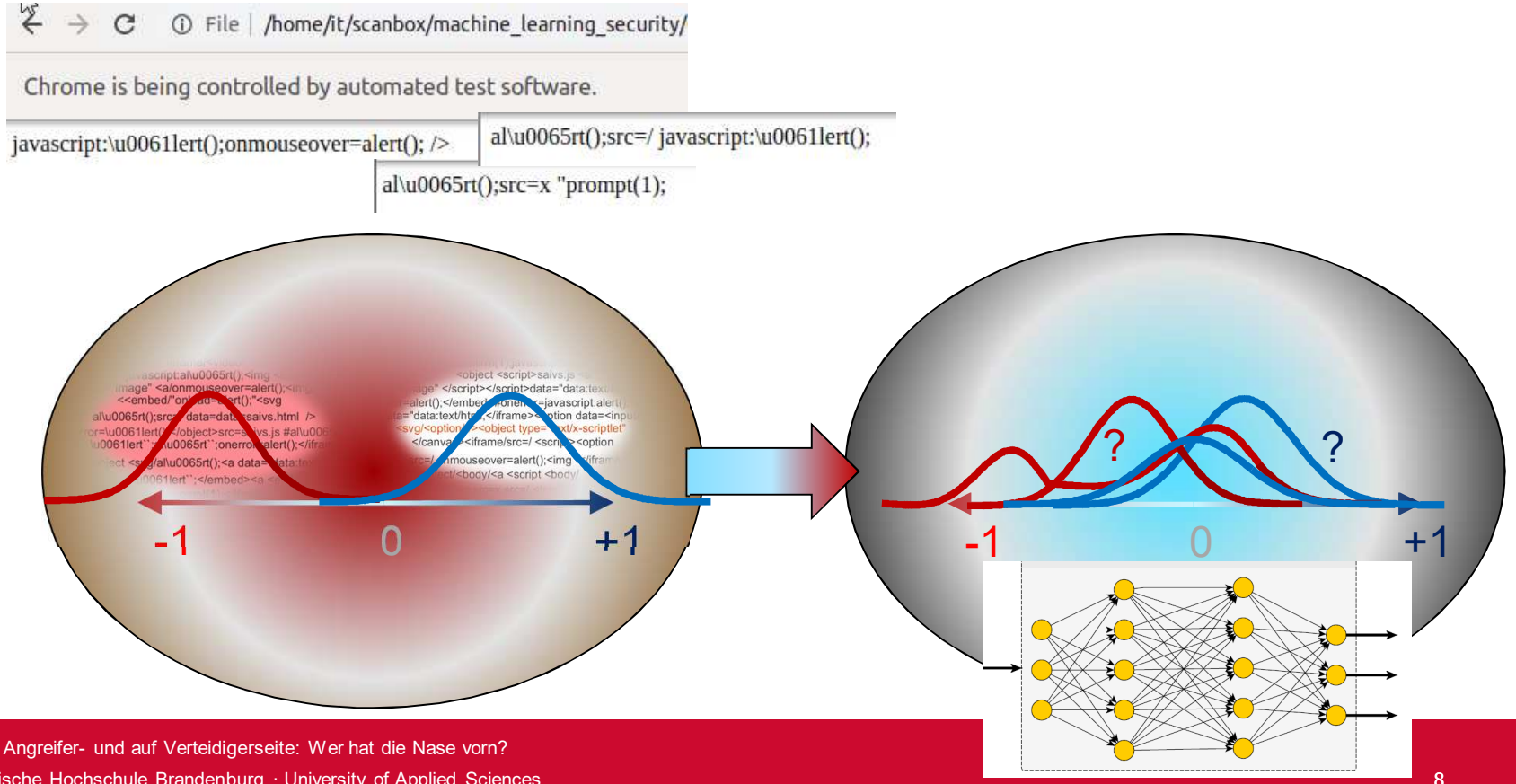
KI für Verteidigung

- Angriffe und Harmloses, jeweils deklariert
- Verteidigung muss lernen zu unterscheiden



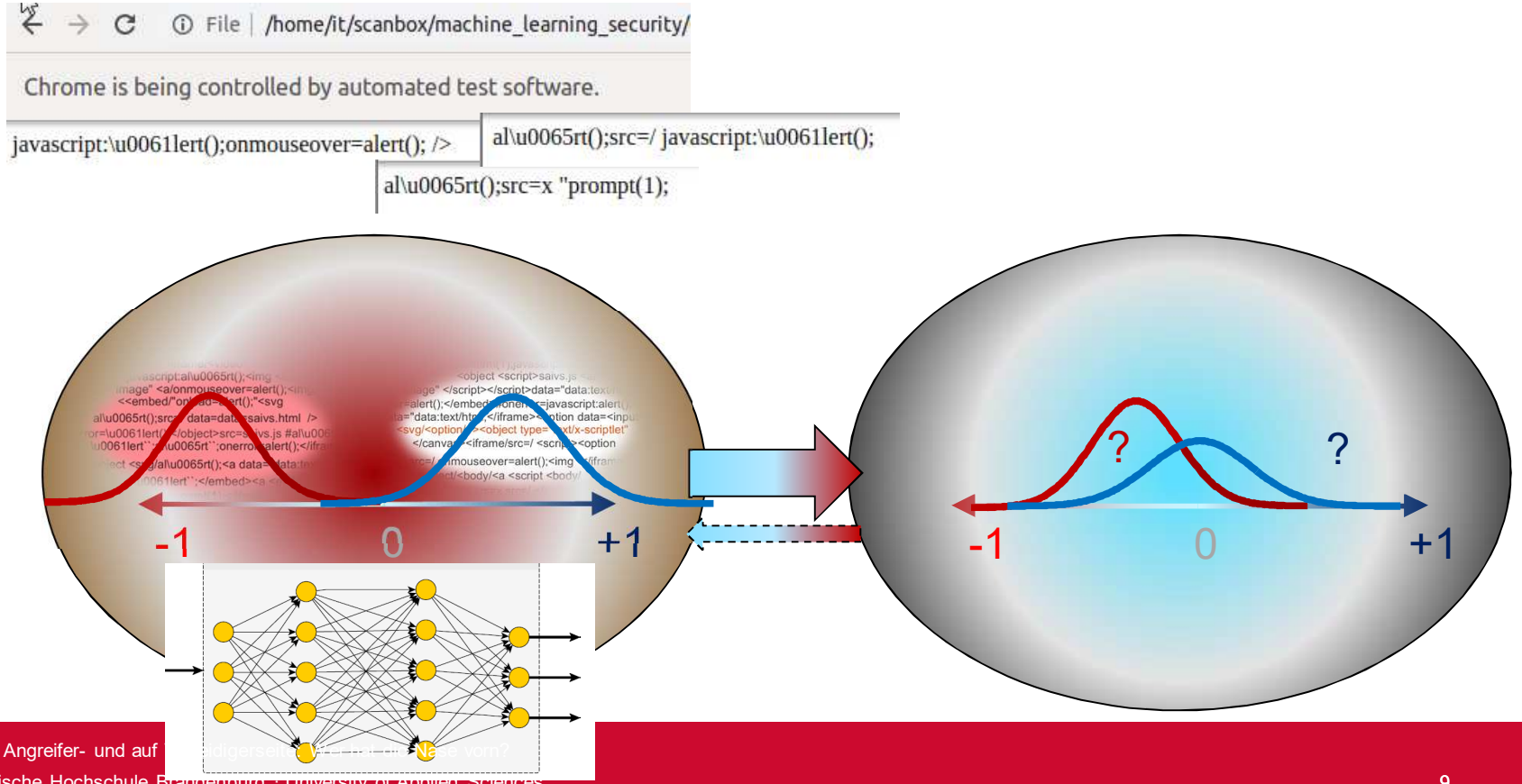
KI für Verteidigung: IDS

- Angriffe und Harmloses, jeweils deklariert
- Verteidigung muss lernen zu unterscheiden



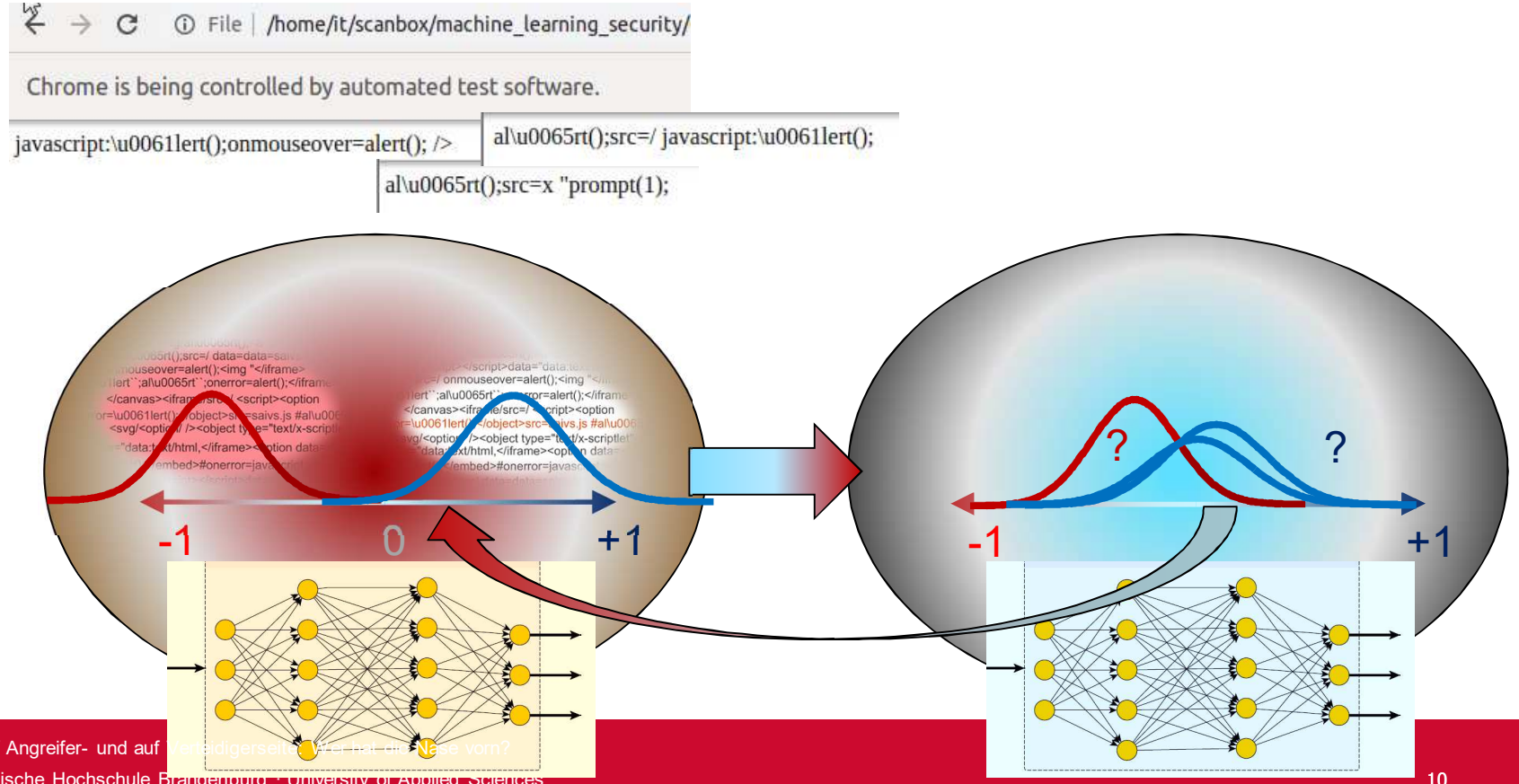
KI für Angriff: Exploit

- Was bleibt unterm Radar?
- Verteidigung beobachten – wie?



KI für Angriff und für Verteidigung: GAN (Generative Advisorial Networks)

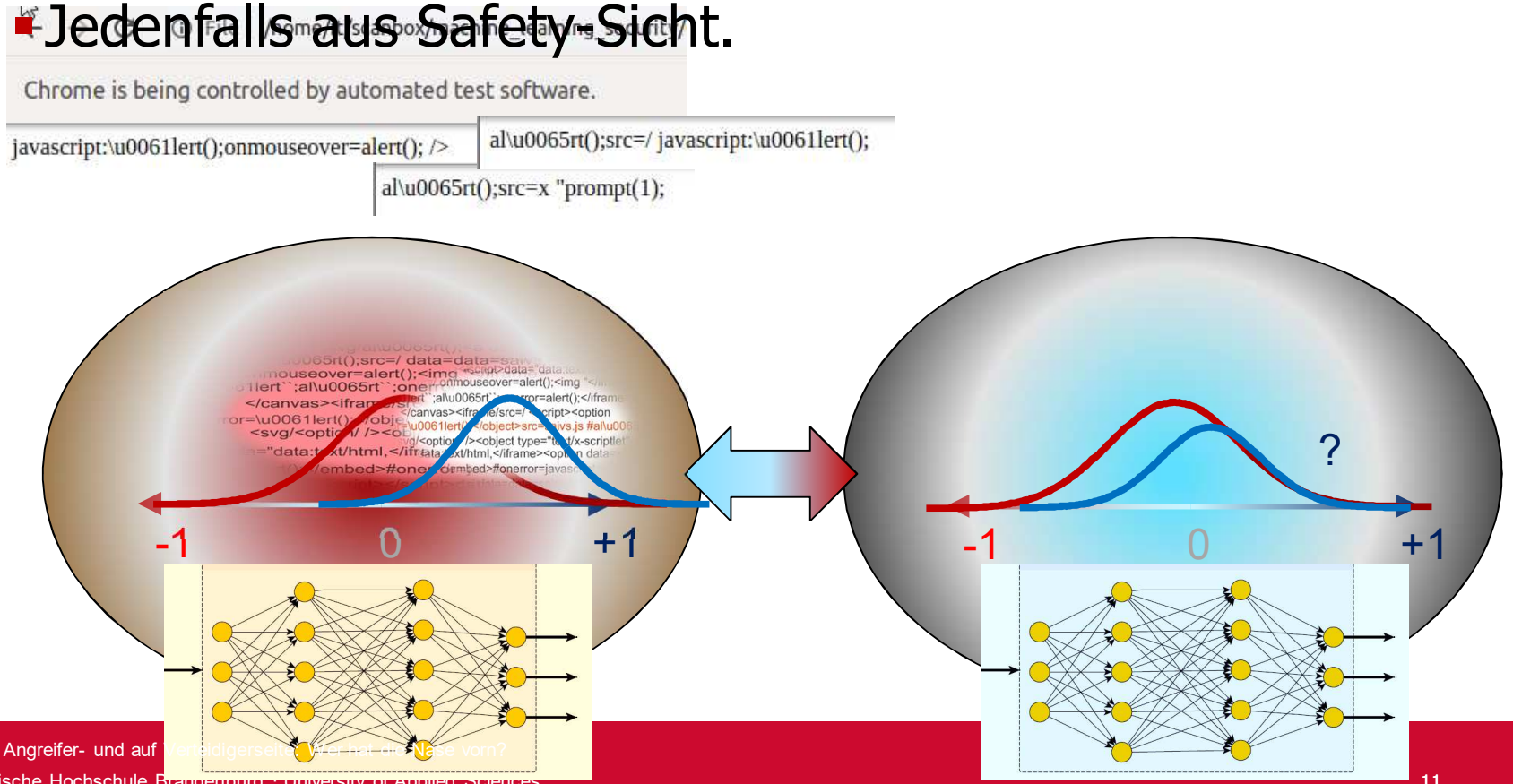
- Beide Seiten gleichzeitig trainieren
- Verstärkte Angriffe dort, wo Verteidigung schwach



KI auf Angreifer- und auf Verteidigerseite

Wer hat die Nase vorn?

- Der Schnellere.
- Jedenfalls aus Safety-Sicht.

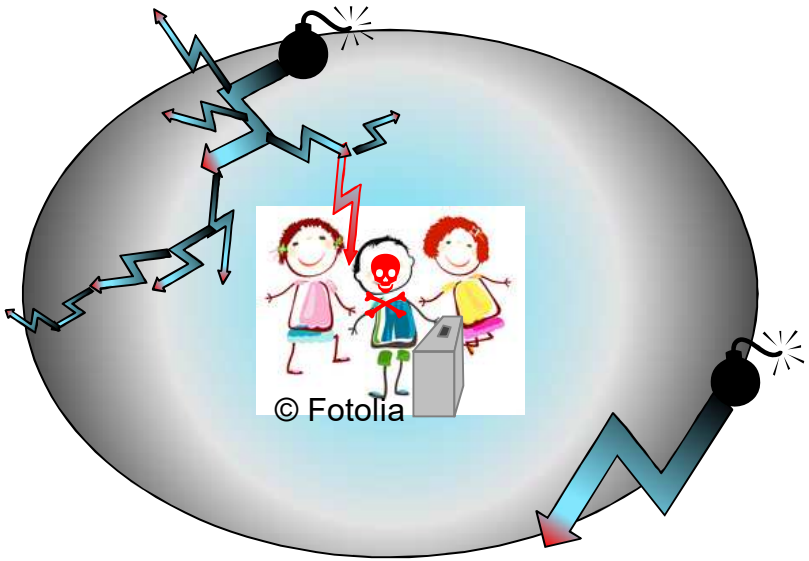


Einschub: Safety-Analyse

- Safety – Schutz des Menschen vorm System
  - Fehlersuche…

    mit vielen, vielen False Positves

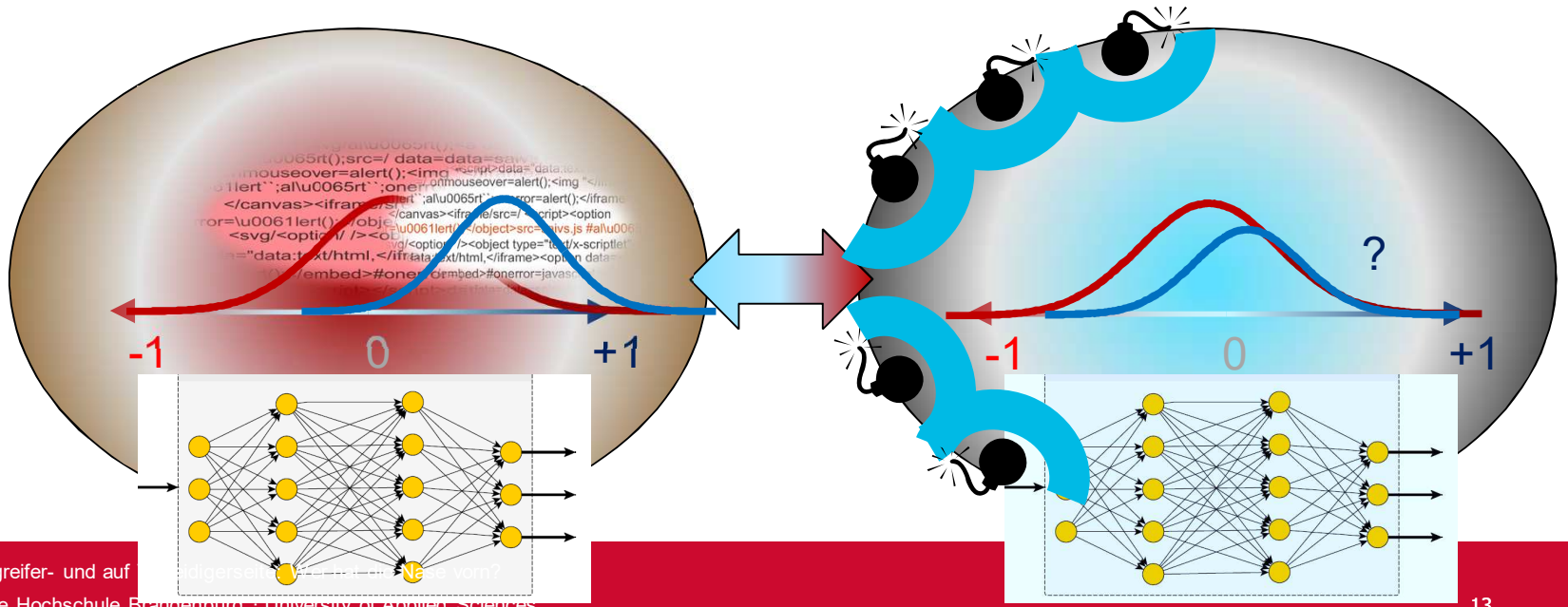
```
root@kali:~# nmap -sV -O 192.168.56.102

Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-09 21:43 CDT
Nmap scan report for 192.168.56.102
Host is up (0.00026s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-
1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/...)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
443/tcp  open  ssl/http    Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-
1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/...)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
5001/tcp open  ovm-manager Oracle VM Manager
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp open  http        Jetty 6.1.25
MAC Address: 08:00:27:3F:C5:C4 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at http://
Nmap done: 1 IP address (1 host up) scanned in 14.14 seconds
```



KI auf Angreifer- und auf Verteidigerseite

Wer hat die Nase vorn?

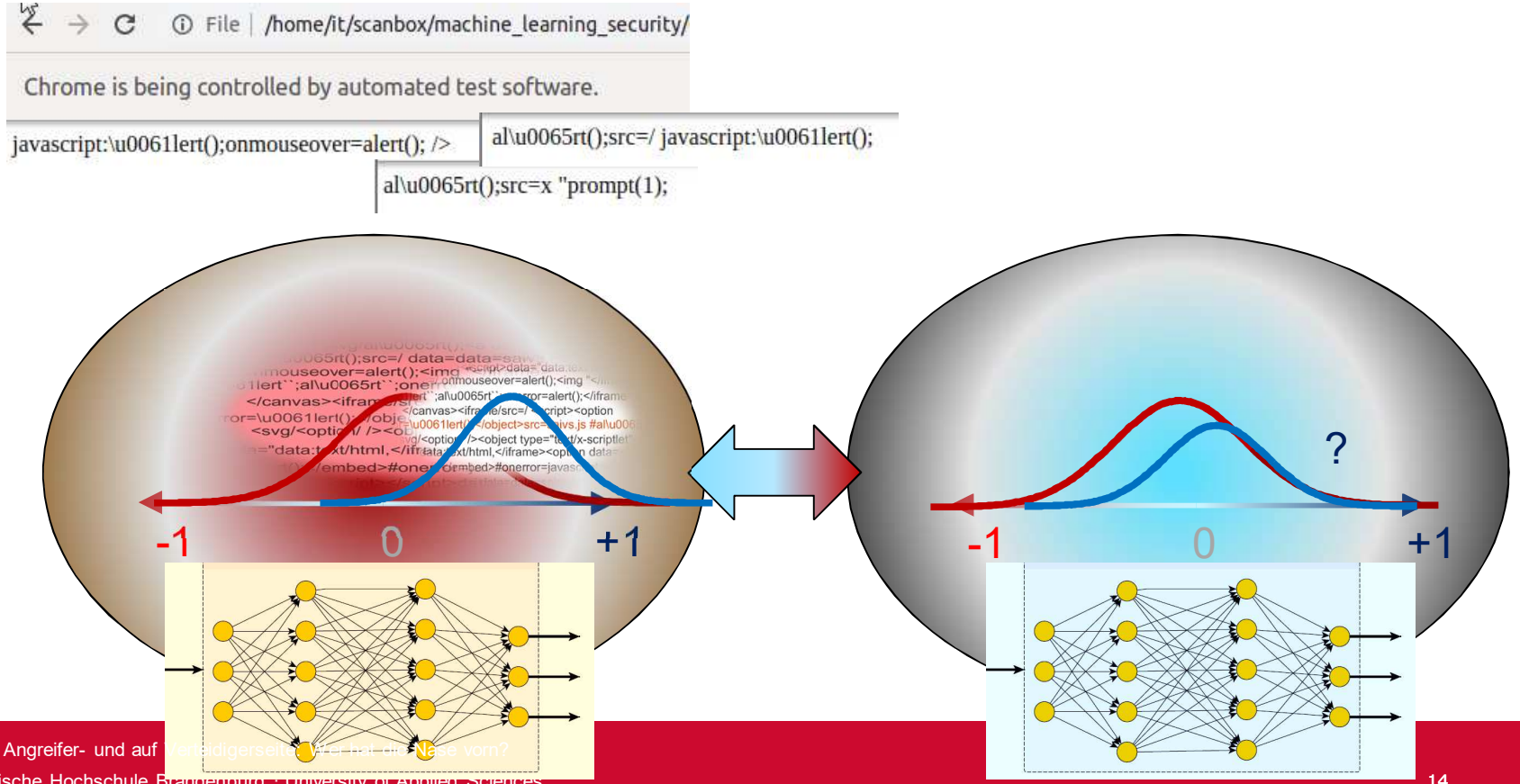
- Aus Safety-Sicht: der Schnellere.
- Da die Verteidigung vereinheitlicht werden muss, während der Angreifer unbegrenzt neue Wege sucht.



KI auf Angreifer- und auf Verteidigerseite

Wer hat die Nase vorn?

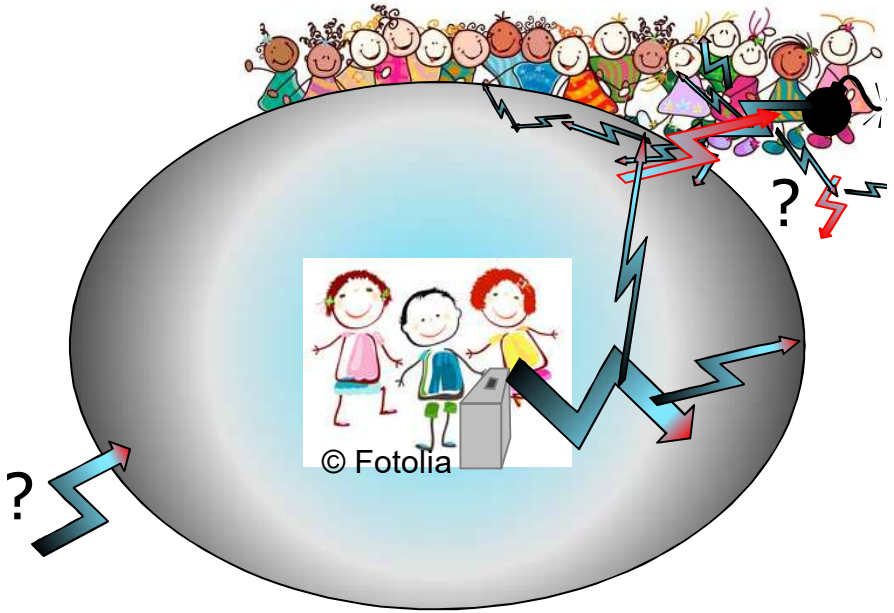
- Aus Security-Sicht: beide?



Einschub: Security-Analyse

- Security – Schutz des Systems (vorm Menschen)
- Selbstschutz

  nach Schutzbedarf: Werte? Angreifer? System?

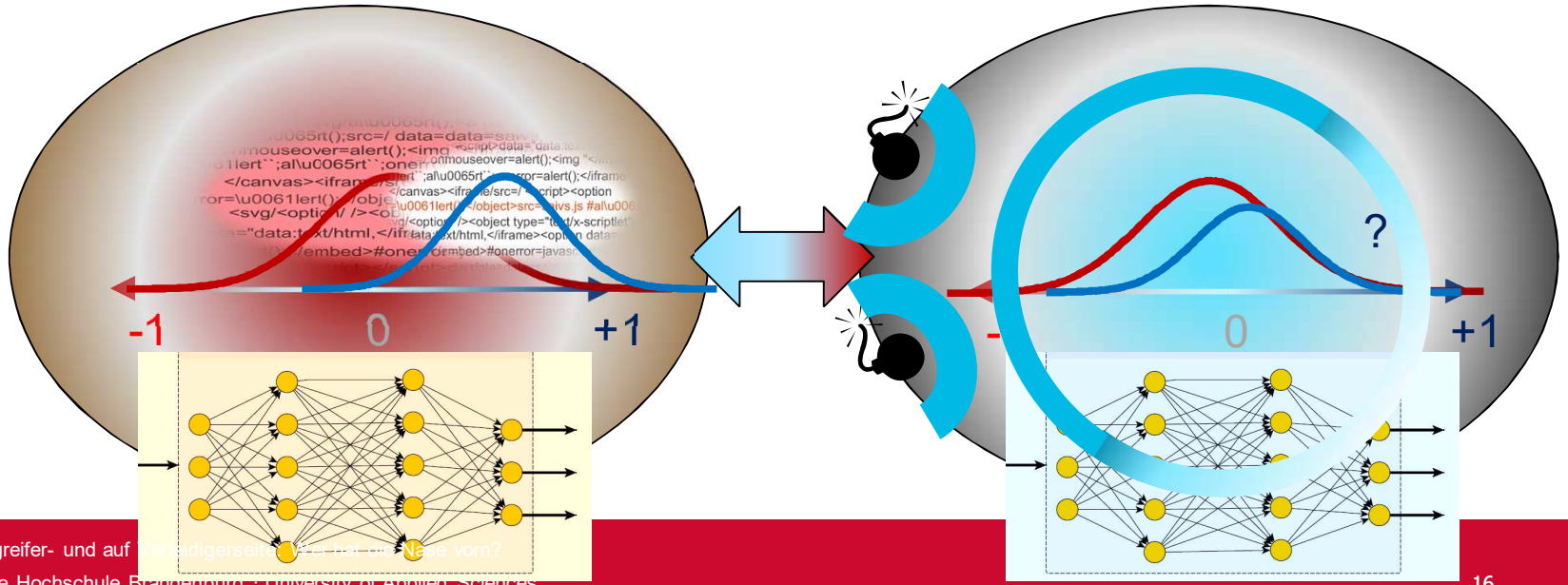


KI auf Angreifer- und auf Verteidigerseite

Wer hat die Nase vorn?

- Aus Security-Sicht: beide.
- Effektiv, da die wahrscheinlichen Angriffspfade gesichtert werden.

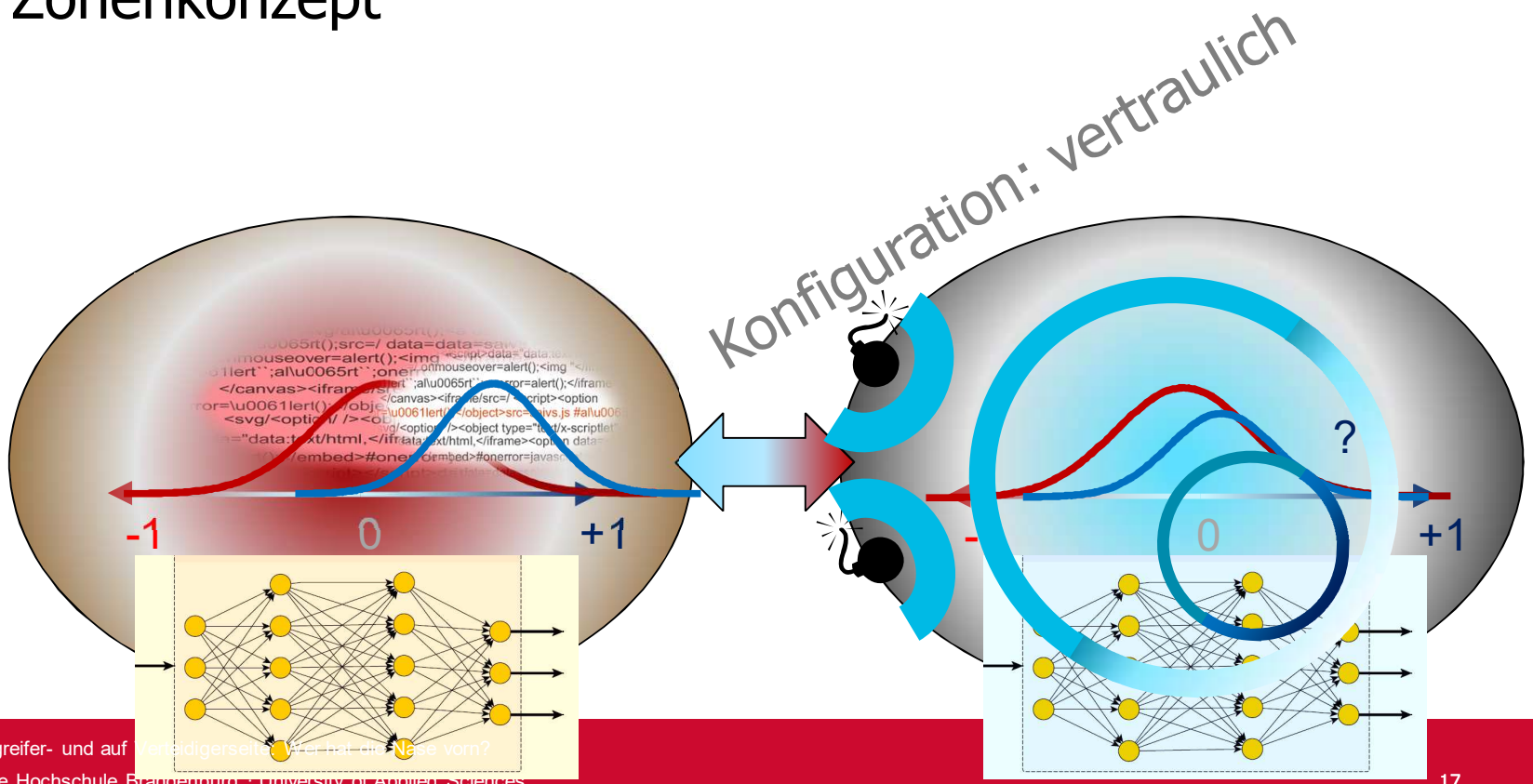
  Was immer der Angreifer so planen mag.



KI auf Angreifer- und auf Verteidigerseite

Wer hat die Nase vorn?

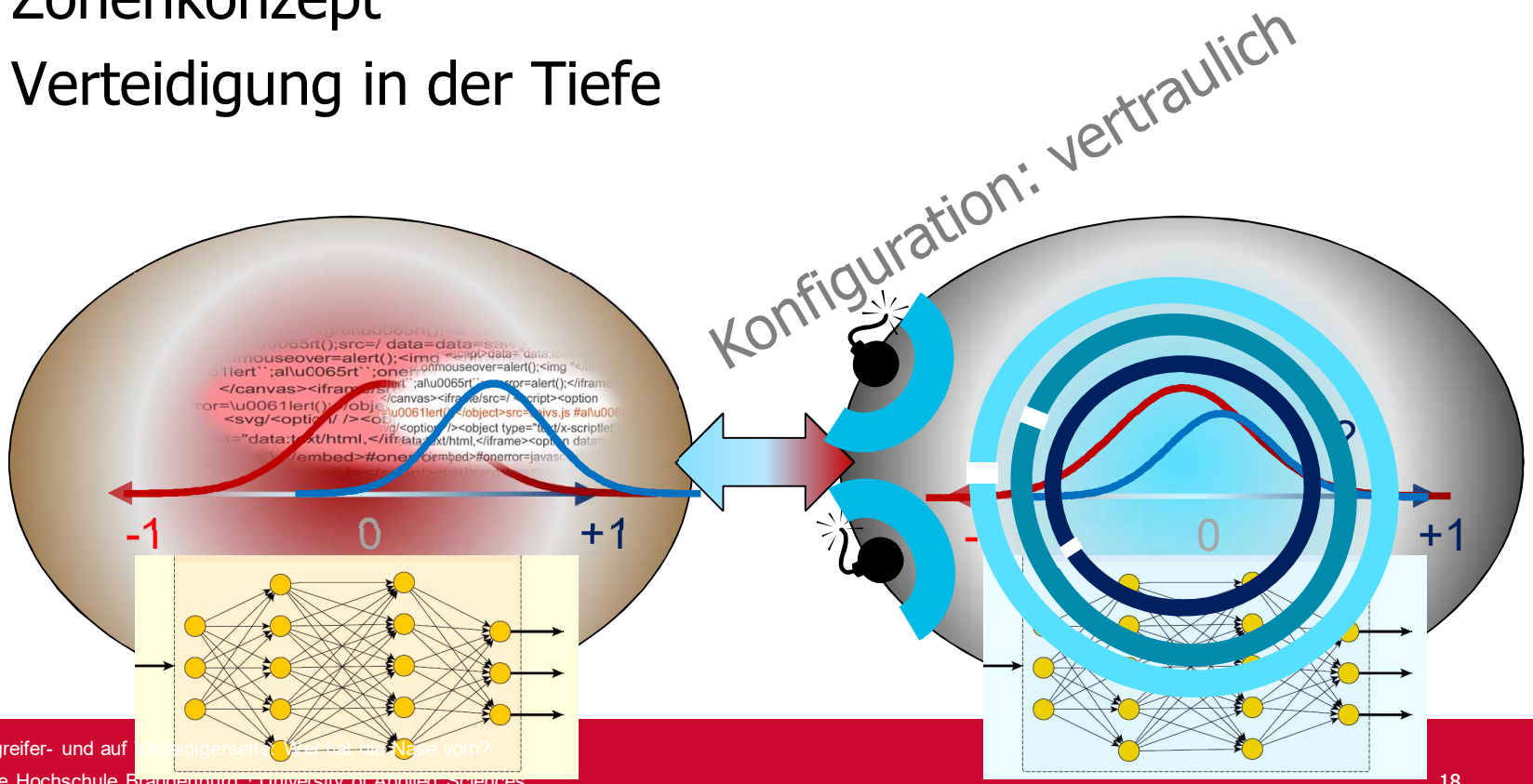
- Aus Security-Sicht: beide.
- Zonenkonzept



KI auf Angreifer- und auf Verteidigerseite

Wer hat die Nase vorn?

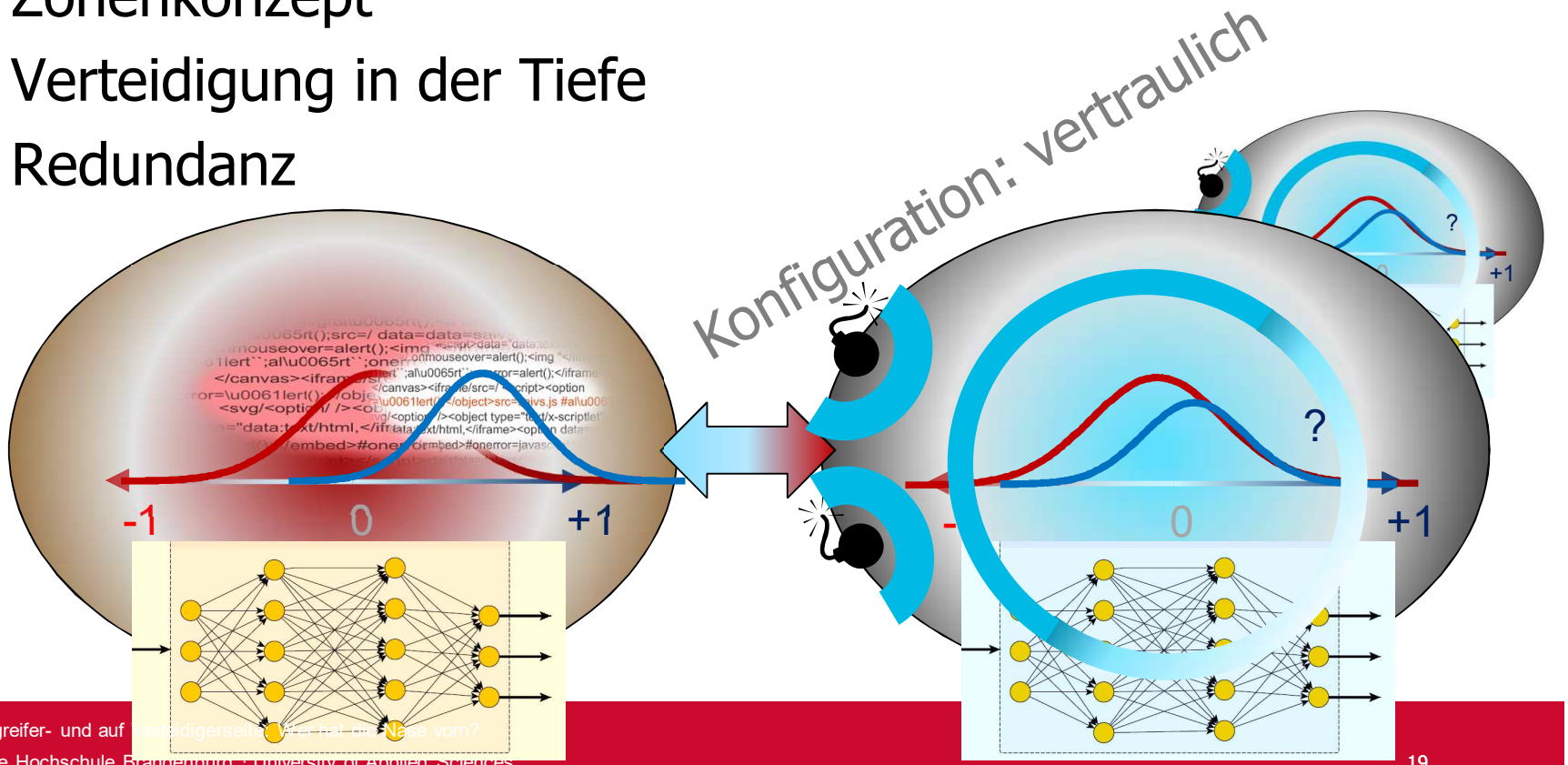
- Aus Security-Sicht: beide.
- Zonenkonzept
- Verteidigung in der Tiefe



KI auf Angreifer- und auf Verteidigerseite

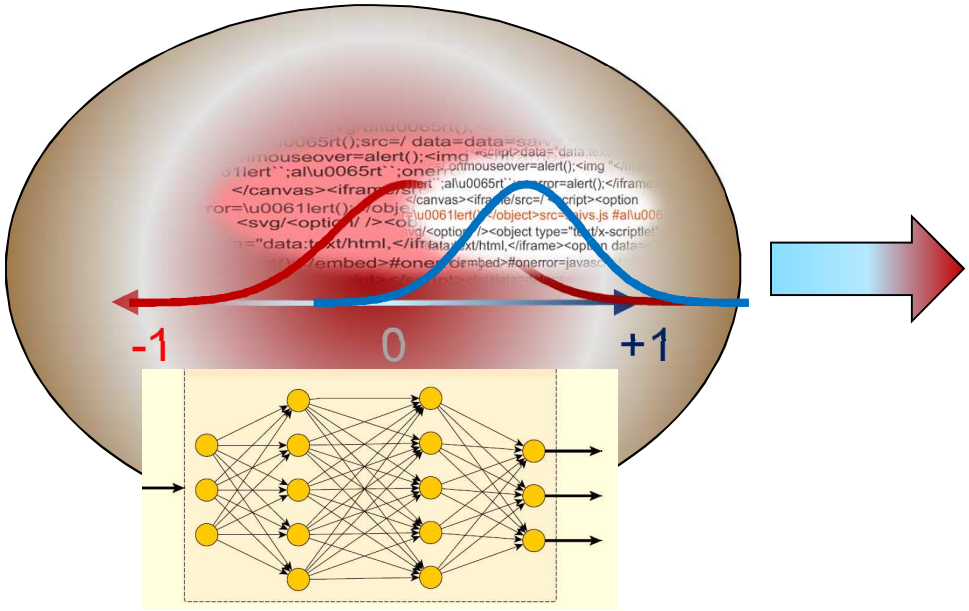
Wer hat die Nase vorn?

- Aus Security-Sicht: beide.
- Zonenkonzept
- Verteidigung in der Tiefe
- Redundanz

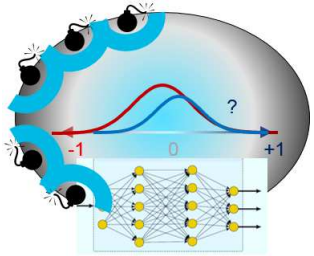


KI auf Angreifer- und auf Verteidigerseite

Wer hat die Nase vorn?

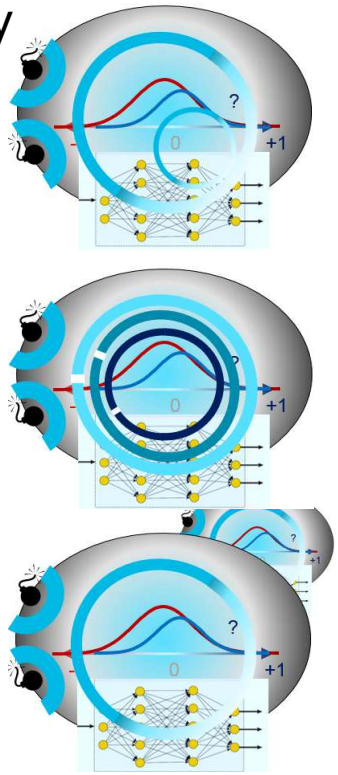


Safety



Security

Konfiguration: vertraulich



Technische Hochschule
Brandenburg
University of
Applied Sciences

KI auf Angreifer- und auf Verteidigerseite: **Wer hat die Nase vorne?**

Danke.

10.1-205, ScanBox

Ivo Keller* und Dragoljub Milasinovic
*Studiengangsdekan *Security Management (M. Sc.)*
TH Brandenburg
keller@th-brandenburg.de, +49 3381 355-278