

100 PX

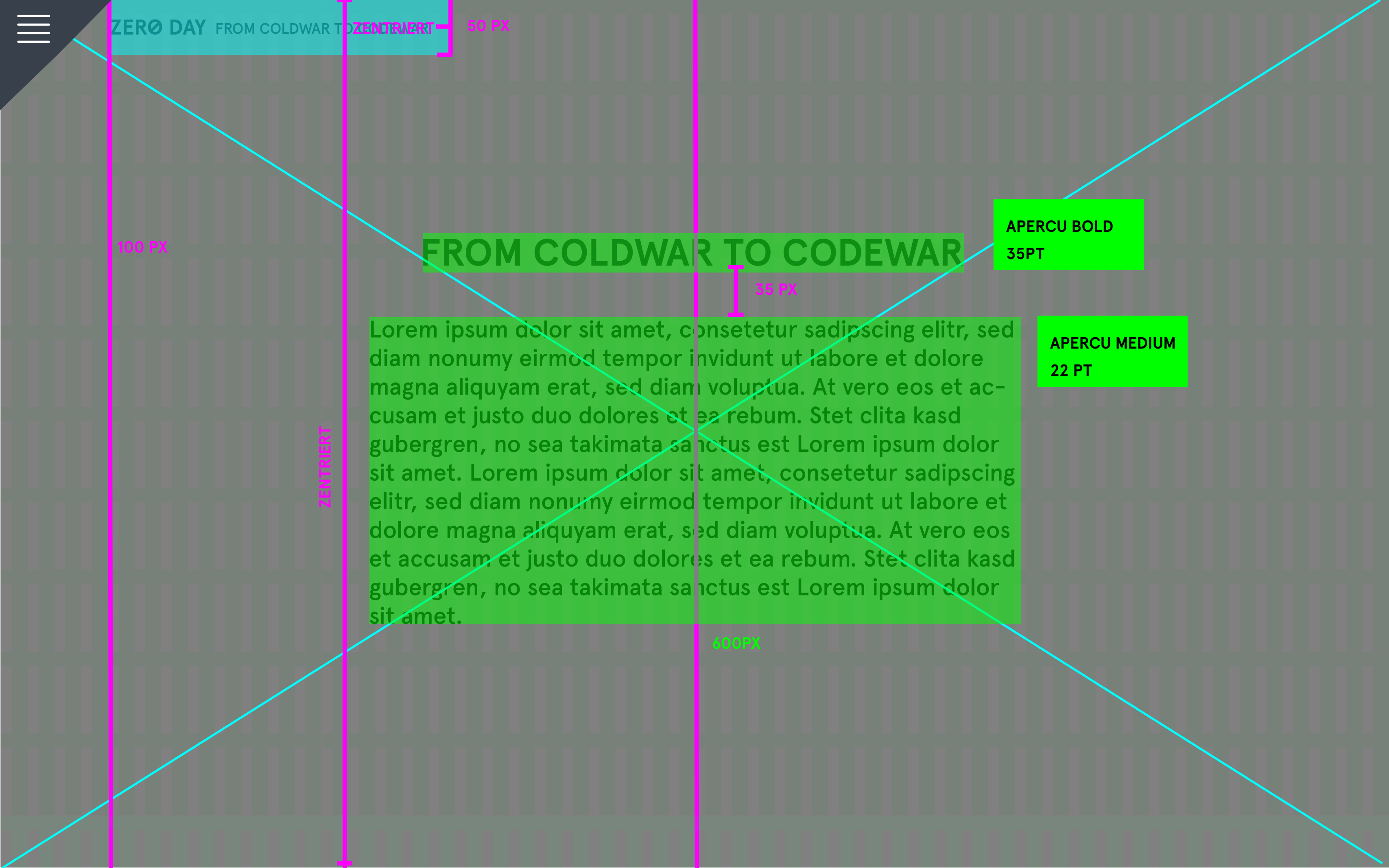
100 PX

460PX

120PX

ZERO DAY
FROM COLDWAR TO CODEWAR





ZERO DAY FROM COLDWAR TO CODEWAR

ZENTRIERT

50 PX

100 PX

FROM COLDWAR TO CODEWAR

35 PX

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

600PX

APERCU BOLD

35PT

APERCU MEDIUM

22 PT

ZENTRIERT



ZERO DAY FROM COLDWAR TO CODEWAR

RGB

192 | 255 | 217

RGB

128 | 255 | 179

RGB

64 | 255 | 141

RGB

0 | 255 | 105

237,5 PX

475,5 PX

25%

25%

APERCU BOLD
28 PT

VIRTUAL WARFARE

REAL IMPACTS

50 PX

CURRENT ATTCAKS

POTENTIAL THREATS



ZENTRIERT

OVERVIEW

APERCU BOLD
70 PT

15 PX

VIRTUAL WARFARE

REAL IMPACTS

CURRENT ATTACKS

POTENTIAL THREATS

APERCU BOLD
25 PT
LINE-HIGHT: 28 PT

30 PX

ABOUT

30 PX

SOURCES

30 PX

IMPRINT



37.5 %

ZENTRIERT

APERCU BOLD
28 PT
LINE-HEIGHT: 28PT

VIRTUAL WARFARE
DAS VIRTUELLE SCHLACHTFELD

50 PX

APERCU MEDIUM
20 PT
LINE-HEIGHT: 22PT

REAL IMPACTS

CURRENT ATTCAKS

POTENTIAL



RGB

128 | 255 | 179

25 PX

APERCU BOLD
35 PT
LINE-HEIGHT: 28PT

100 PX

VIRTUAL WARFARE
DAS VIRTUELLE SCHLACHTFELD

200PX

APERCU MEDIUM
20 PT
LINE-HEIGHT: 22PT





WEIß

TRANSPARENZ 90%

200 PX

WAS IST CYBERWAR?

150 PX

APERCU BOLD

35 PT

APERCU MEDIUM

18 PT

35 PX

300 PX

Seit mehr als einem Jahrzehnt wird über Cyberwar debattiert. Medien tendieren dazu, den Begriff für sämtliche digitale Attacken zu verwenden. Populäre Beispiele sind der NSA-Abhörskandal »Regin« oder das AKW-Sabotage-Projekt »Stuxnet«. Zahlreiche Hacking-Angriffe wie jene auf das Weisse Haus, auf die Homepage Estlands oder auf Nachrichtenportale wie Le Monde nach »Charlie Hebdo« wurden zu Cyberwar-Akten erklärt.



Unterschiedliche Cyberwar-Experten haben versucht den Begriff Cyberwar zu definieren. Sie kommen zum Teil zu verschiedenen Ergebnissen. In einem Punkt sind sie sich aber einig. Cyberwar-Angriffe gehen immer von Staaten aus und sie haben das Ziel sich einen politischen und militärischen Vorteil zu verschaffen. Cyberwar im engeren Sinn hat das Ziel gegnerische Staaten mit Gewalt und Zerstörung zu besiegen. Diese Art von Cyberwar hat bis heute nicht stattgefunden.

APERCU MEDIUM

22 PT



Dagegen gehen von zivilen Cyberattacken zumeist deutlich geringere Bedrohungen aus. Sie können nach Angreifer-Typ und Angriffsziel unterschieden werden. Da gibt es den »Teenagerhacker«, der aus Lust an der technischen Herausforderung in sensible Datensysteme einbricht. Zweitens gibt es die politischen Aktivisten, die in einer Art virtueller Sitzblockade Internetseiten von kritisierten Organisationen oder Unternehmen blockieren oder verändern. Und es gibt drittens »Cybercrime«, bei dem es darum geht, dass sich Einzelpersonen oder Organisationen durch Cyberattacken einen illegalen wirtschaftlichen Nutzen verschaffen. Das beginnt bei Kleinkriminellen, die Kontodaten ausspähen und geht bis zu groß angelegter Unternehmensspionage.



WAS MEINEN DIE EXPERTEN?

Klicke auf die Experten

P.W. Singer

Politikwissenschaftler



WAS MEINEN DIE EXPERTEN?

Hover über die Experten!

»Whether it be war on land, at sea, or in the air, or now in cyberspace, war always has a political goal and mode (which distinguishes it from crime) and always has an element of violence [...] the effect must be physical damage or destruction. [...] Knowing when cyberwar begins or ends, however, might be more challenging than defining it. [...]«

P.W. Singer

Politikwissenschaftler



WAS ÄNDERT SICH AN DER KRIEGSFÜHRUNG?

»Der Aufmarsch wird lautlos sein. Kein Panzer rollt, keine Geschütze donnern, keine Flieger dröhnen durch die Luft. Nur Tastaturklappern und Mausklicks – so klingt der Krieg der Zukunft.« – Christian Bartlau.

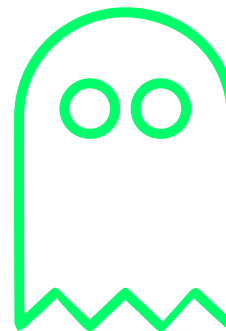
Cyberwar unterscheidet sich wesentlich von konventioneller Kriegsführung. Die spezifischen Möglichkeiten von Cyberattacken verändern die Bedingungen für Angreifer wie für Angegriffene.



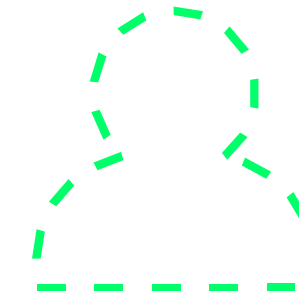
CHARAKTERISTIKAS DER NEUEN KRIEGSFÜHRUNG



**KRIEG OHNE
RAUM UND ZEIT**



**UNSICHTBARE
ANGRIFFE**



**ATTRIBUTATIONS-
PROBLEM**



**GERINGES RISIKO
KLEINES GELD**



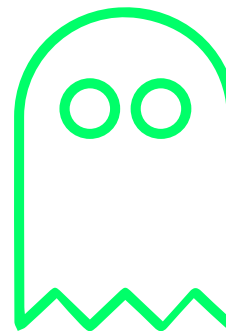
**HOHE HACKER-
KOMPETENZ**



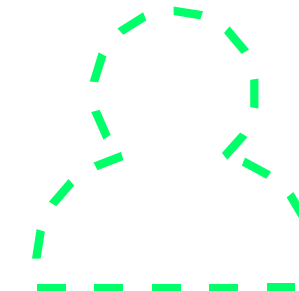
CHARAKTERISTIKAS DER NEUEN KRIEGSFÜHRUNG



**KRIEG OHNE
RAUM UND ZEIT**



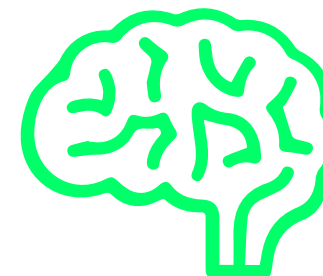
**UNSICHTBARE
ANGRIFFE**



**ATTRIBUTATIONS-
PROBLEM**



**GERINGES RISIKO
KLEINES GELD**



**HOHE HACKER-
KOMPETENZ**



DER KRIEG OHNE RAUM UND ZEIT

Das neue an Cyberwar-Angriffen ergibt sich aus ihren technischen Möglichkeiten. Während konventionelle militärische Angriffe immer eindeutig räumlich und zeitlich zugeordnet werden können, ist dies bei Cyberwar-Attacken nicht immer möglich. Wenn eine Bombe auf ein Haus fällt, ist das Angriffsziel eindeutig bestimmt und der Angriffsweg kann zu- meist zeitlich und räumlich rückverfolgt werden.

KRIEG OHNE
RAUM UND ZEIT

Dies ist bei Cyberwar-Attacken nicht immer so. Ein Vieren- angriff kann schon Jahre vor dem Schadensfall erfolgt sein. Der zeitliche Zusammenhang mit der Schadenswirkung kann in aller Regel nicht mehr hergestellt werden. Auf der anderen Seite können sich Angriffe mit Lichtgeschwindigkeit im Netz verbreiten, oder gar zeitgleich in mehreren Zielsystemen stattfinden. Auch der Zielort ist nicht immer eindeutig, da ja nicht das physisch zerstörte Ziel direkt angegriffen wird, sondern ein IT-System, das das physische Zielesystem steuert. So kann z.B. ein Angriff auf die Zentrale der deutschen Hochspannungsnetze in Hamburg dafür sorgen, dass in München die Stromversorgung ausfällt.

ATTRIBUTATIONS-
PROBLEM



WAS MEINEN DIE EXPERTEN?

»Sie kommen heimlich und bleiben manchmal jahrelang, ohne entdeckt zu werden. Ein Mausklick genügt, um sie zu aktivieren und die Kontrolle zu übernehmen. Wanzen, Würmer, Viren – die Waffen im Zeitalter der digitalen Kriegsführung.«

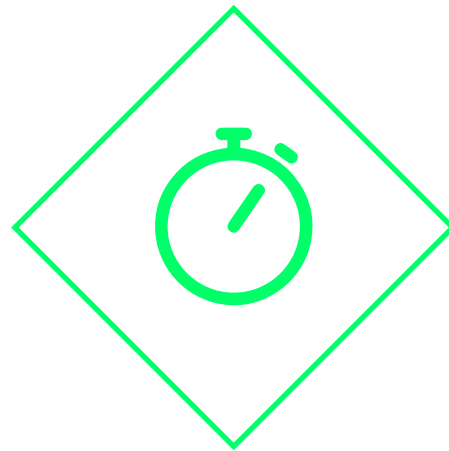
Malte Herwig

Politikwissenschaftler





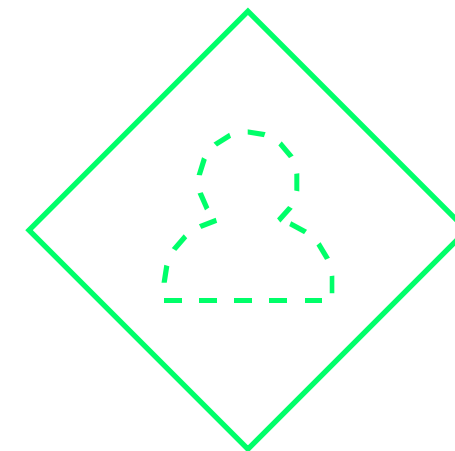
CHARAKTERISTIKAS DER NEUEN KRIEGSFÜHRUNG



**KRIEG OHNE
RAUM UND ZEIT**



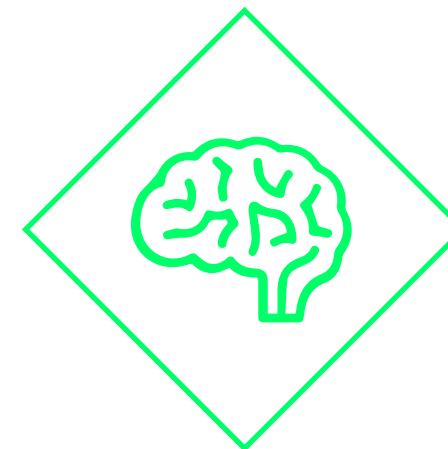
**UNSICHTBARE
ANGRIFFE**



**ATTRIBUTATIONS-
PROBLEM**



**GERINGES RISIKO
KLEINES GELD**



HACKER SKILLS



UNSICHTBARE ANGRIFFE

Cyberwar-Angriffe sind besonders effektiv, wenn sie möglichst lange unbemerkt bleiben. Deshalb wird ein hoher Aufwand betrieben um im angegriffenen System unsichtbar zu bleiben. Dies wird dadurch erreicht, dass eine einmal eingedrungene Schadsoftware sich für lange Zeit in den Ruhemodus legen kann und dann durch externe Signale aktiviert wird, oder es zerstört sich nach erfolgreicher Manipulation des Zielsystems selbst. Noch komplexere Unsichtbarkeitsstrategien beeinflussen die IT-Überwachungssysteme oder die physikalischen Überwachungssysteme der Zielsysteme. So wird selbst die physische Zerstörung des Zielsystems erst bemerkt, wenn keine Gegenmaßnahmen mehr möglich sind.

Noch raffinierte könnten Angriffe wirken, die als „stiller Ruin“ bezeichnet werden. Hierbei soll die Wirtschaftsunternehmen, Infrastruktur, Informationsstruktur etc. eines Landes so angegriffen werden, dass ihre Effizienz ständig sinkt. Die Angriffe dürfen hier nicht als Angriffe erkannt werden. Vielmehr erscheinen die Probleme als System-Fehler, Fehlentscheidungen oder menschliches Versagen. Die Wirtschaftskraft eines Landes kann damit aber nachhaltig geschwächt werden.



ATTRIBUTATIONS-
PROBLEM





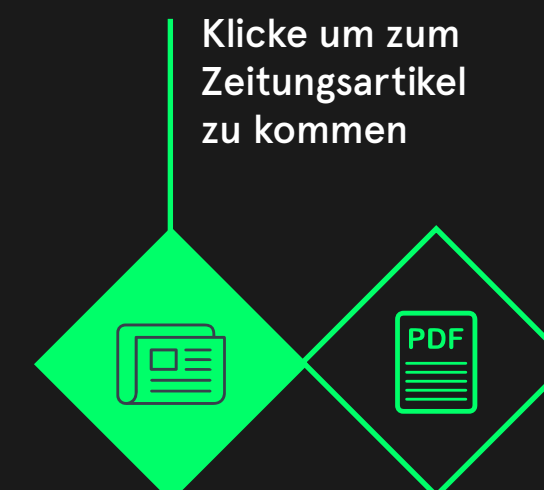
UNSICHTBARE ANGRIFFE

Cyberwar-Angriffe sind besonders effektiv, wenn sie möglichst lange unbemerkt bleiben. Deshalb wird ein hoher Aufwand betrieben um im angegriffenen System unsichtbar zu bleiben. Dies wird dadurch erreicht, dass eine einmal eingedrungene Schadsoftware sich für lange Zeit in den Ruhemodus legen kann und dann durch externe Signale aktiviert wird, oder es zerstört sich nach erfolgreicher Manipulation des Zielsystems selbst. Noch komplexere Unsichtbarkeitsstrategien beeinflussen die IT-Überwachungssysteme oder die physikalischen Überwachungssysteme der Zielsysteme. So wird selbst die physische Zerstörung des Zielsystems erst bemerkt, wenn keine Gegenmaßnahmen mehr möglich sind.

Noch raffinierte könnten Angriffe wirken, die als „stiller Ruin“ bezeichnet werden. Hierbei soll die Wirtschaftsunternehmen, Infrastruktur, Informationsstruktur etc. eines Landes so angegriffen werden, dass ihre Effizienz ständig sinkt. Die Angriffe dürfen hier nicht als Angriffe erkannt werden. **Vielmehr erscheinen die Probleme als System-Fehler, Fehlentscheidungen oder menschliches Versagen.** Die Wirtschaftskraft eines Landes kann damit aber nachhaltig geschwächt werden.



ATTRIBUTATIONS-
PROBLEM



Klicke um zum
Zeitungsartikel
zu kommen



WAS MEINEN DIE EXPERTEN?

»Zudem suchte Stuxnet auch nach weiteren geeigneten Systemen zu Infektion unter Ausnutzung der sogenannten Autorun-Funktion von Windows. Stuxnet löscht sich nach einer bestimmten Zahl von erfolgreichen Infektionen selbst.«

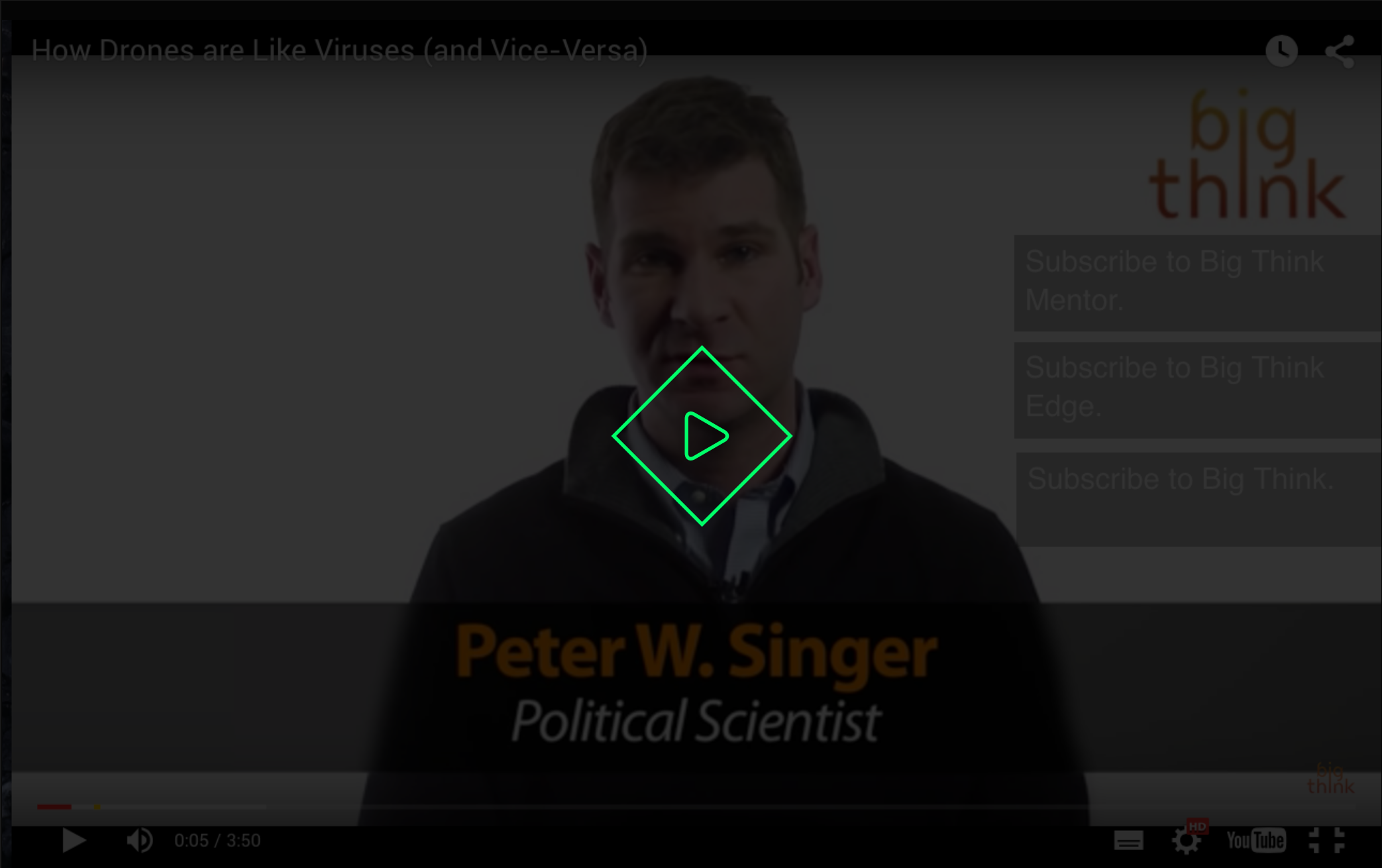
Prof. Dr. Dr. K. Saalbach
Politikwissenschaftler





INTERVIEW MIT P. W. SINGER ZUM NEUEN KRIEGSFÜHRUNG

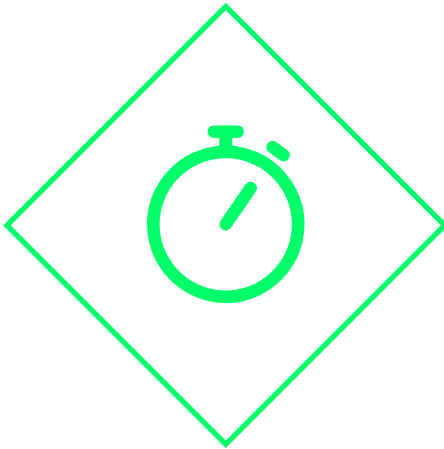
How Drones are Like Viruses (and Vice-Versa)



Peter W. Singer
Political Scientist

0:05 / 3:50

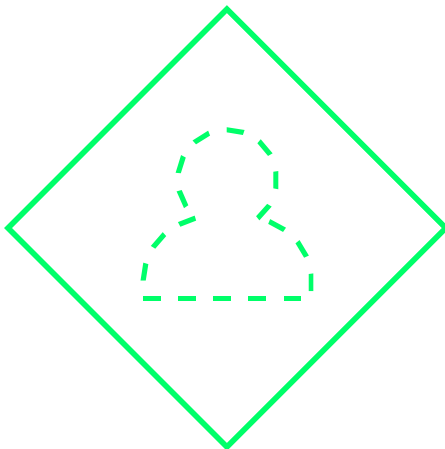
Noch raffinierte
könnten Angriffe
wirken, die als „stil-
ler Ruin“ bezeichnet



KRIEG OHNE
RAUM UND ZEIT



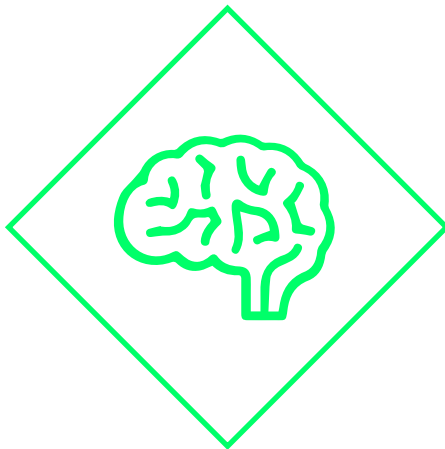
UNSICHTBARE
ANGRIFFE



ATTRIBUTATIONS-
PROBLEM

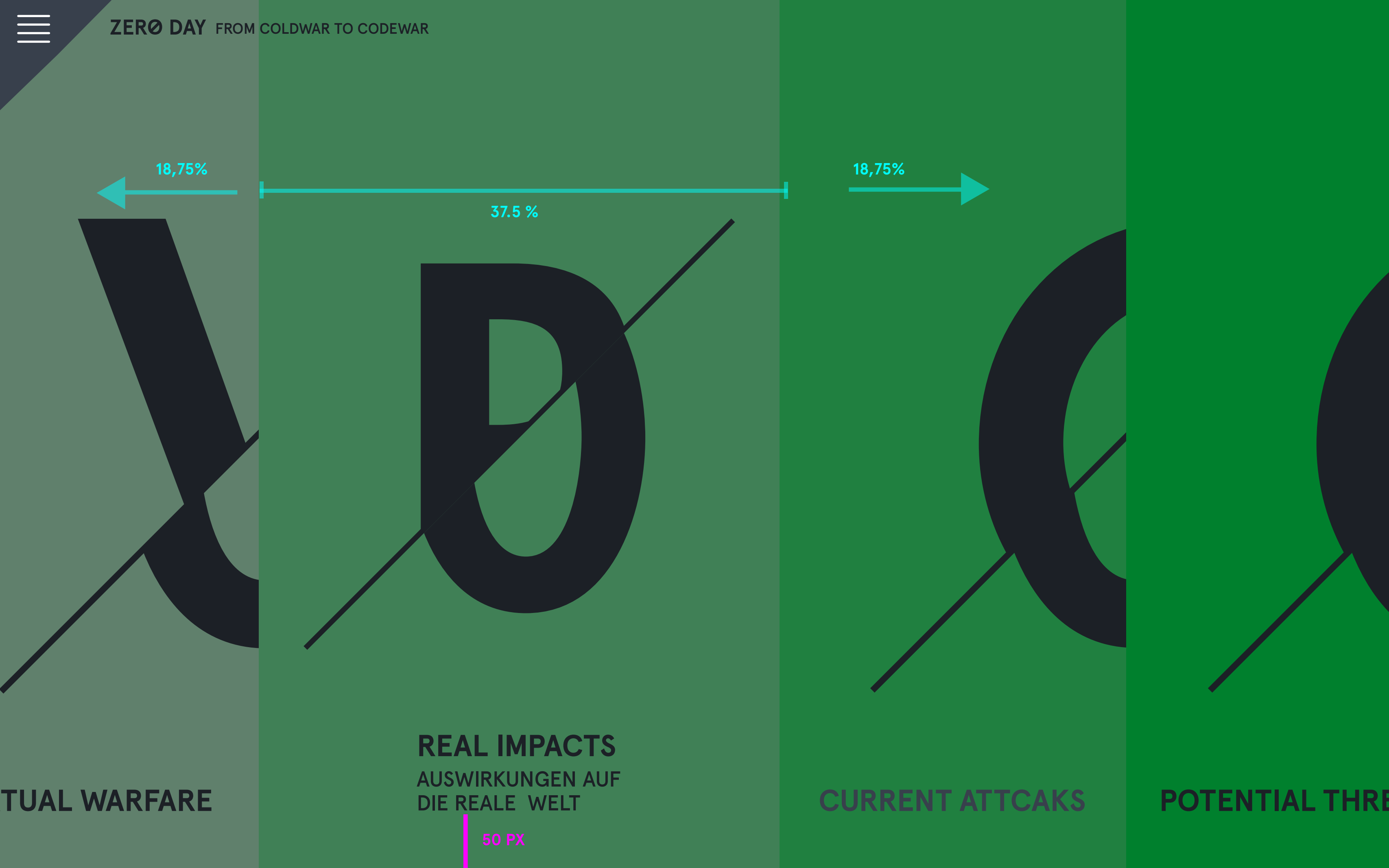


GERINGES RISIKO
KLEINES GELD



HACKER SKILLS





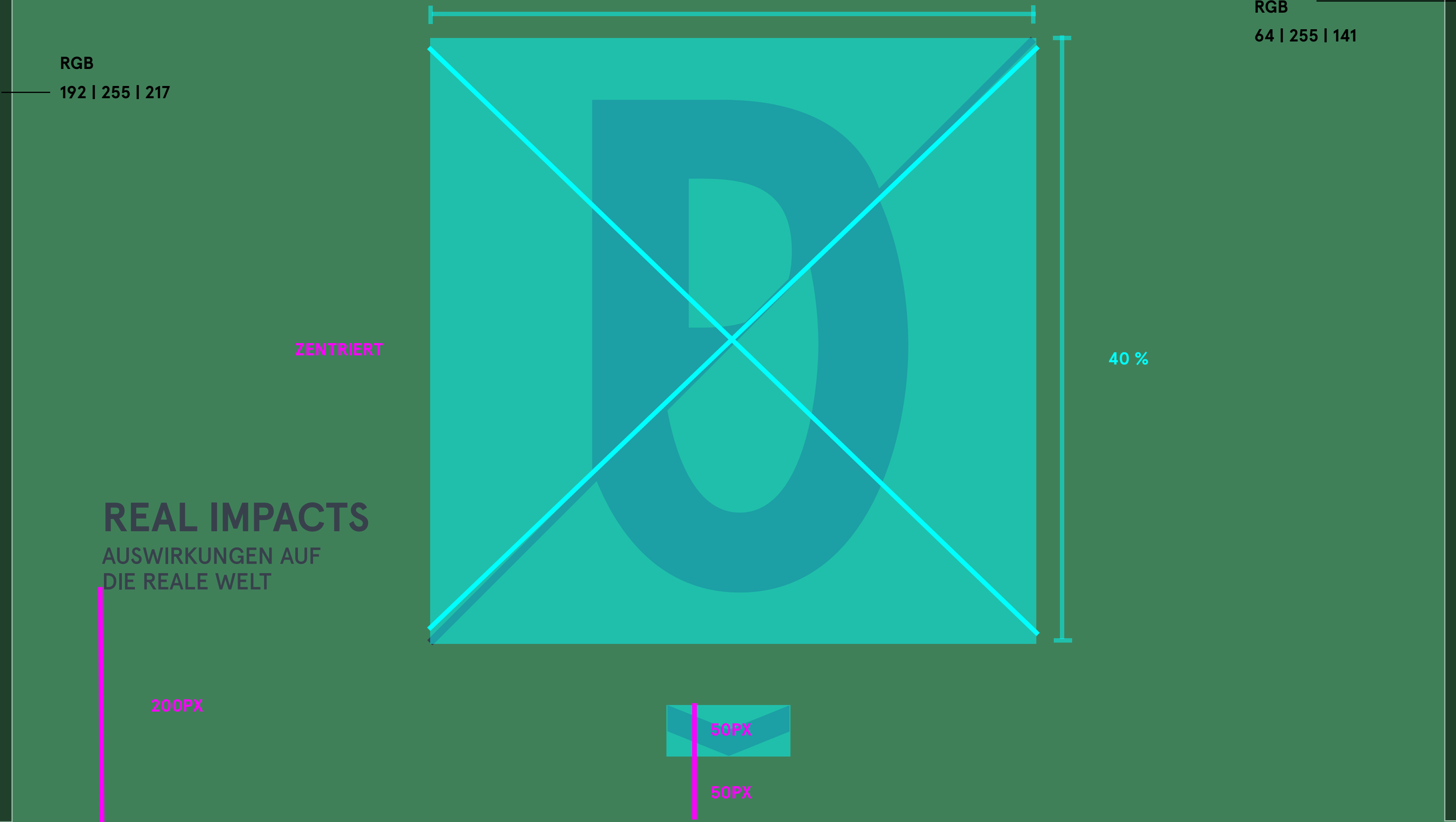
ACTUAL WARFARE

REAL IMPACTS

AUSWIRKUNGEN AUF
DIE REALE WELT

CURRENT ATTACKS

POTENTIAL THREATS



VIRTUALISIERUNG DER WELT

»Die eigentliche Bedrohung sind nicht Hacker und Cyber-Krieger, sondern die zunehmende Virtualisierung der Welt.«

– Marcel Kolvenbach

Cyberwar-Attacken greifen mit digitalen Methoden digitale Ziel-Systeme an. Die Wirkungen dieser virtuellen Angriffe bleiben aber nicht auf die virtuelle Welt beschränkt. Unsere reale, physische Welt hat sich immer stärker in die Abhängigkeit einer virtuellen Parallelwelt begeben. Informationsmedien, Wirtschaft und Finanzströme und kritische Infrastrukturen werden heute von digitalen Systemen gesteuert. Ein Ausfall solcher Systeme, oder deren Manipulation kann zu großen Schäden in der realen Welt führen.

Die Vernetzung dieser digitalen Steuerungssysteme und insbesondere deren Einbindung in das Internet machen sie zum Teil der virtuellen Parallelwelt. Cyberwar-Attacken können so zu



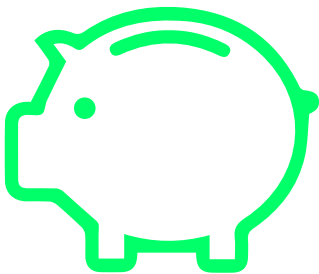
ABHÄNGIGKEIT VON VERNETZEN SYSTEMEN

Die reale Bedrohung durch Cyberwar-Attacken wird erst verständlich, wenn unsere Abhängigkeit von vernetzten Systemen und deren Verwundbarkeit deutlich wird.



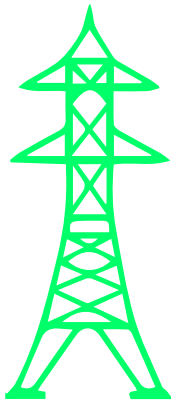
MEDIEN & INFORMATION

Lorem ipsum dolor sit amet, consetetur sadipseirmor.



WIRTSCHAFT & FINANZMARKT

Nonumy eirmod tempor invidunt ut labore et dolor.



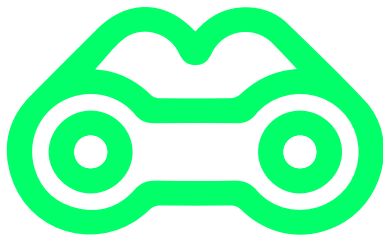
KRITSCHKE INFRASTRUKTUR

Consetetur sadips-cing elitr, sed diam nonumy eirmod tempor invidun.



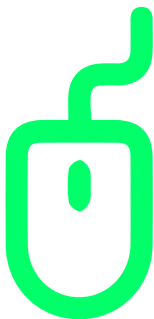
ART DER VERWUNDBARKEITEN

Cyberwar im engeren Sinn hat das Ziel gegnerische Staaten mit Gewalt und Zerstörung zu besiegen. Diese Art von Cyberwar hat bis heute nicht stattgefunden.



SPIONAGE

Lorem ipsum dolor sit amet, consetetur sadipseirmor.



MANIPULATION

Nonumy eirmod tempor invidunt ut labore et dolor.



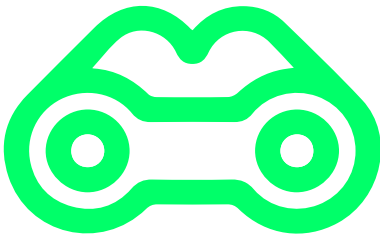
SABOTAGE

Consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidun.





Cyberwar im engeren Sinn hat das Ziel gegnerische Staaten mit Gewalt und Zerstörung zu besiegen. Diese Art von Cyberwar hat bis heute nicht stattgefunden.



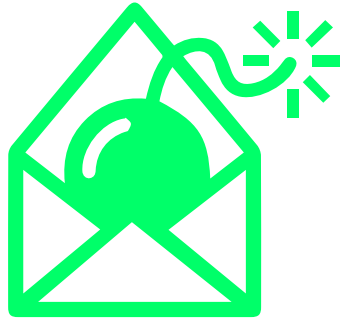
SPIONAGE

Lorem ipsum dolor sit amet, consetetur sadipseirmor.



MANIPULATION

Nonumy eirmod tempor invidunt ut labore et dolor.



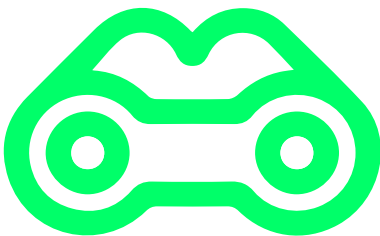
SABOTAGE

Consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidun.





Cyberwar im engeren Sinn hat das Ziel gegnerische Staaten mit Gewalt und Zerstörung zu besiegen. Diese Art von Cyberwar hat bis heute nicht stattgefunden.



SPIONAGE

Lorem ipsum dolor sit amet, consetetur sadipseirmor.



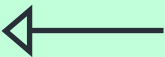
MANIPULATION

Nonumy eirmod tempor invidunt ut labore et dolor.



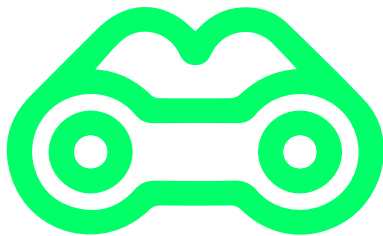
SABOTAGE

Consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidun.



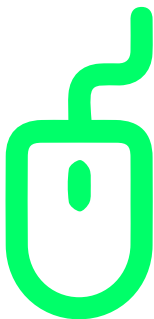
ART DER VERWUNDBARKEITEN

Cyberwar im engeren Sinn hat das Ziel gegnerische Staaten mit Gewalt und Zerstörung zu besiegen. Diese Art von Cyberwar hat bis heute nicht stattgefunden.



SPIONAGE

Lorem ipsum dolor sit amet, consetetur sadipseirmor.



MANIPULATION

Nonumy eirmod tempor invidunt ut labore et dolor.



SABOTAGE

Consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidun.



TUAL WARFARE



REAL IMPACTS



CURRENT ATTACKS
DIE GESCHICHTE DER
CYBERATTACKEN



POTENTIAL THRE



CURRENT ATTACKS

DIE GESCHICHTE DER
CYBERATTACKEN





DIE GECSHICHTE DER CYBERATTACKEN

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.





2015

- 2014
- 2013
- 2012
- 2011
- 2010
- 2009
- 2008
- 2007
- 2006
- 2005
- 2004
- 2003
- 2002
- 2001
- 2000
- 1999
- 1998
- 1982

APRIL 7
12 AM





2015

- 2014
- 2013
- 2012
- 2011
- 2010
- 2009
- 2008
- 2007
- 2006
- 2005
- 2004
- 2003
- 2002
- 2001
- 2000
- 1999
- 1998
- 1982

APRIL 7
12 AM





2015 | APRIL 7 12:00 AM
ALLJÄHLICHE HACKERATTACKE

Seit 2013 ist der 7. April Tag der Cyberangriffe. In diesem Jahr wurden offenbar mehrere israelische Webseiten angegriffen, darunter zahlreiche Seiten der Regierung. Hinter den Angriffen stecken anscheinend propalästinensische Hacker, bei Twitter bekannte sich ein Kollektiv namens Op_Israel zu den virtuellen Angriffen. Unter dem freien Kollektiv Anonymous kann praktisch jeder im Internet Hackerangriffe starten. Die Organisation Op_Israel protestierte schon durch frühere Angriffe gegen Entscheidungen der israelischen Regierung.

APRIL 7
12 AM

2015

- 2014
- 2013
- 2012
- 2011
- 2010
- 2009
- 2008
- 2007
- 2006
- 2005
- 2004
- 2003
- 2002
- 2001
- 2000
- 1999
- 1998
- 1997





POTENTIAL THREATS

VERÄNDERUNG DER WELTWEITEN
MACHTKONSTELLATION





DEFINITION „ANTI-ASYMMETRIE“

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.





ERKLÄRUNG MAP

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. et.

COVENTIONAL THREAT





VEREINIGTE STAATEN



CONVENTIONAL THREAT



CODEWAR THREAT



BIP

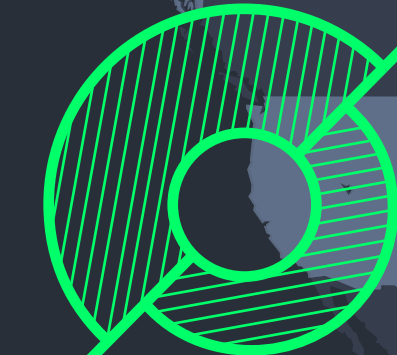


VEREINIGTE STAATEN

CONVENTIONAL THREAT

CODEWAR THREAT

VEREINIGTE STAATEN



- NETWORKING 9.3**
2000000 IP-ADRESSEN
- INFASTRUCTURE 8.9**
345. 098 STROMVERBRAUCH
- OPEN NET 7.9**
8.4 DEMOKRATISIERUNGSINDEX
- CONFLICTS 5.5**
23 KONFLIKTE
- CYBERATTACKS 6.9**
694 372 ZIEL VON CYBERATTACKEN

8.5 CODEWAR POTENTIAL THREAT



INFASTRUCTURE

Der Infrastrukturindex gibt an, wie viel kritische Infrastruktur in einem Land vorhanden ist. Je mehr kritische Infrastruktur, desto größer die Gefahr, dass diese durch virtuelle Attacken gestört werden, was dann zu großen realen Auswirkungen führt.

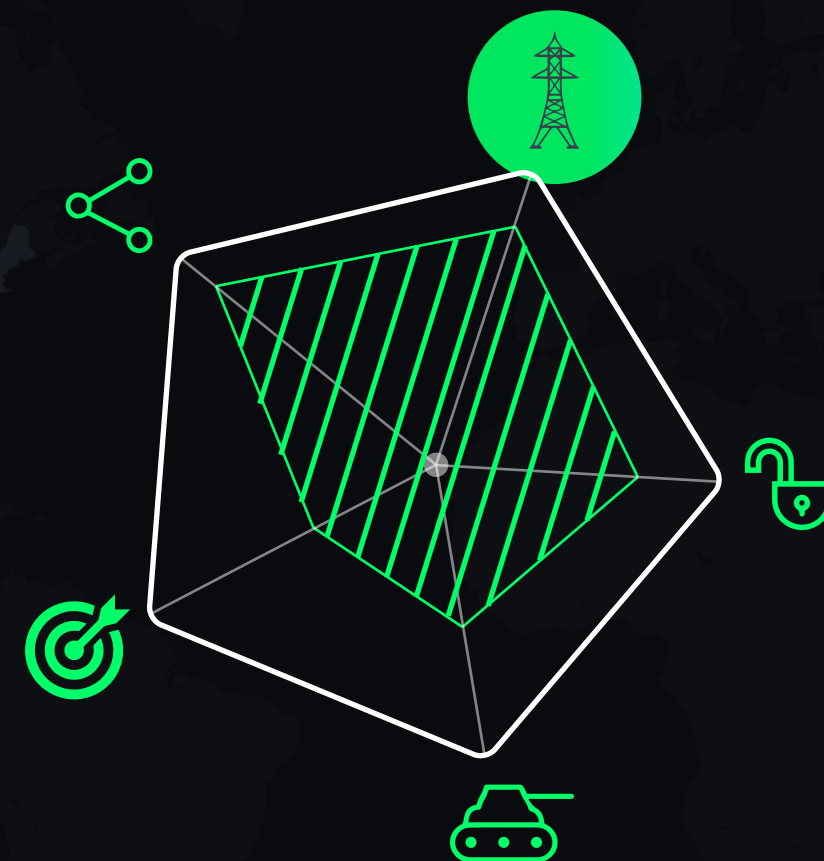
Beispiel:
Wenn die Stromversorgung von New York abgeschaltet wird, ist die Auswirkung größer, als wenn der Strom-Generator in einem afrikanischen Dorf ausgeschaltet wird.

Indikator:
Stromverbrauch pro Einwohner

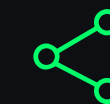
VEREINIGTE STAATEN

CONVENTIONAL THREAT

CODEWAR THREAT



8.5 CODEWAR POTENTIAL THREAT



NETWORKING 9.3

2000000 IP-ADRESSEN



INFASTRUCTURE 8.9

345. 098 STROMVERBRAUCH



OPEN NET 7.9

8.4 DEMOKRATISIERUNGSINDEX



CONFLICTS 5.5

23 KONFLIKTE



CYBERATTACKS 6.9

694 372 ZIEL VON CYBERATTACKEN



CONVENTIONAL THREAT



CODEWAR THREAT



BIP