



ZERO DAY

FROM COLDWAR TO CODEWAR



FROM COLDWAR TO CODEWAR

Cyberwar ist längst kein fiktives »Science-Fiction Szenario« mehr. Durch die zunehmende Anzahl an Cyberangriffen, ausgeführt durch Hacker aus aller Welt, wird der Begriff »Cyberwar« immer häufiger von Medien und IT-Experten als reale Gefahr verstanden. Die Experten reden von Cyberwar allerdings nur, wenn staatliche Akteure beteiligt sind. Tatsächlich bereiten sich die Militärs vieler Staaten mit defensiven und offensiven Strategien auf diese neue virtuelle Gefahrenlage vor.

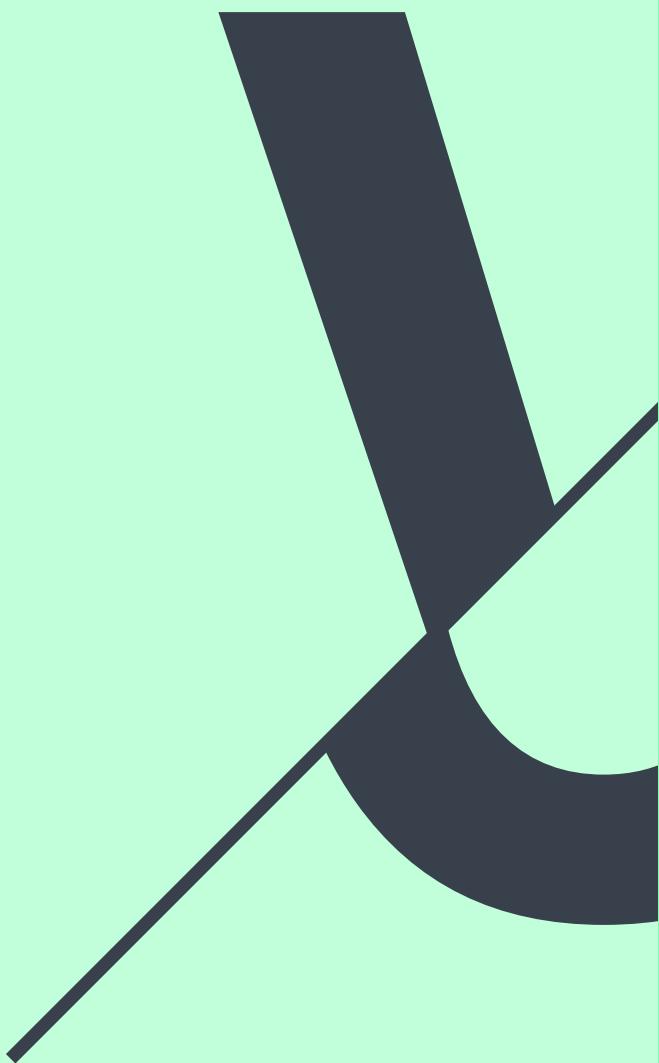
Der Übergang von der konventionellen Art der Kriegsführung (»Coldwar«) zu den neuen Angriffsmöglichkeiten des Cyberwars (»Codewar«) hat aber auch weitreichende politische Konsequenzen. Denn die spezifischen Rahmenbedingungen des Cyberwar könnten auch die weltweiten Machtkonstellationen verändern.

»Zero-Day« bezeichnet den Tag, an dem eine neue IT-Sicherheitslücke auftritt. Wenn ein Hacker diese Lücke nutzt, bevor sie geschlossen werden konnte, wird dies als »Zero-Day-Exploit« bezeichnet. »Zero Day« – Ist der Tag an dem in der virtuellen Welt alle »Einsen« auf »Null« gesetzt werden. Was passiert, wenn damit alle Steuerungsdaten gelöscht werden?



ZERO DAY

VIRTUAL WARFARE



REAL IMPACTS



CURRENT ATTACKS



POTENTIAL THREATS



VIRTUAL WARFARE

REAL IMPACTS

CURRENT ATTACKS

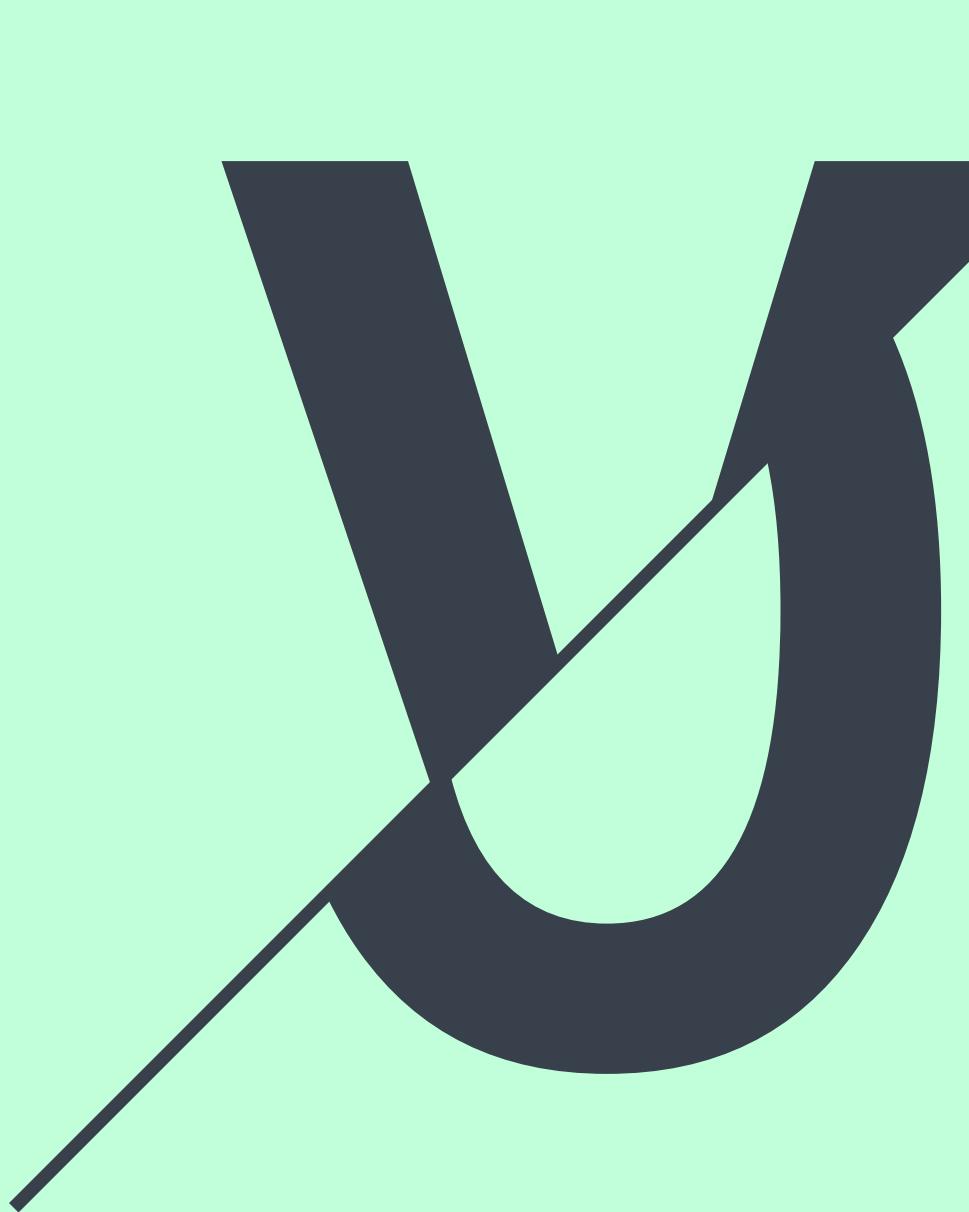
POTENTIAL THREATS

ABOUT

SOURCES



VIRTUAL WARFARE DAS VIRTUELLE SCHLACHTFELD



REAL IMPACTS



CURRENT ATTACKS



POTENTIAL THREATS





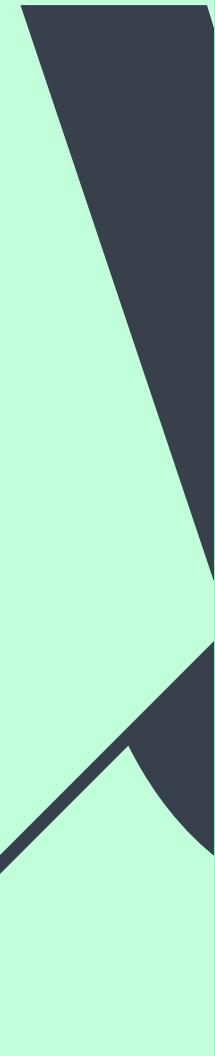
VIRTUAL WARFARE

DAS VIRTUELLE SCHLACHTFELD





VIRTUAL WARFARE



REAL IMPACTS

AUSWIRKUNGEN AUF DIE REALE WELT



CURRENT ATTACKS



POTENTIAL THREATS





REAL IMPACTS
AUSWIRKUNGEN AUF DIE REALE WELT





VIRTUAL WARFARE



REAL IMPACTS



CURRENT ATTACKS
DIE GESCHICHTE DER CYBERATTACKEN



POTENTIAL THREATS



CURRENT ATTACKS

DIE GESCHICHTE DER CYBERATTACKEN





VIRTUAL WARFARE



REAL IMPACTS



CURRENT ATTACKS



POTENTIAL THREATS
VERÄNDERUNG DER WELTWEITEN MACHTKONSTELLATION



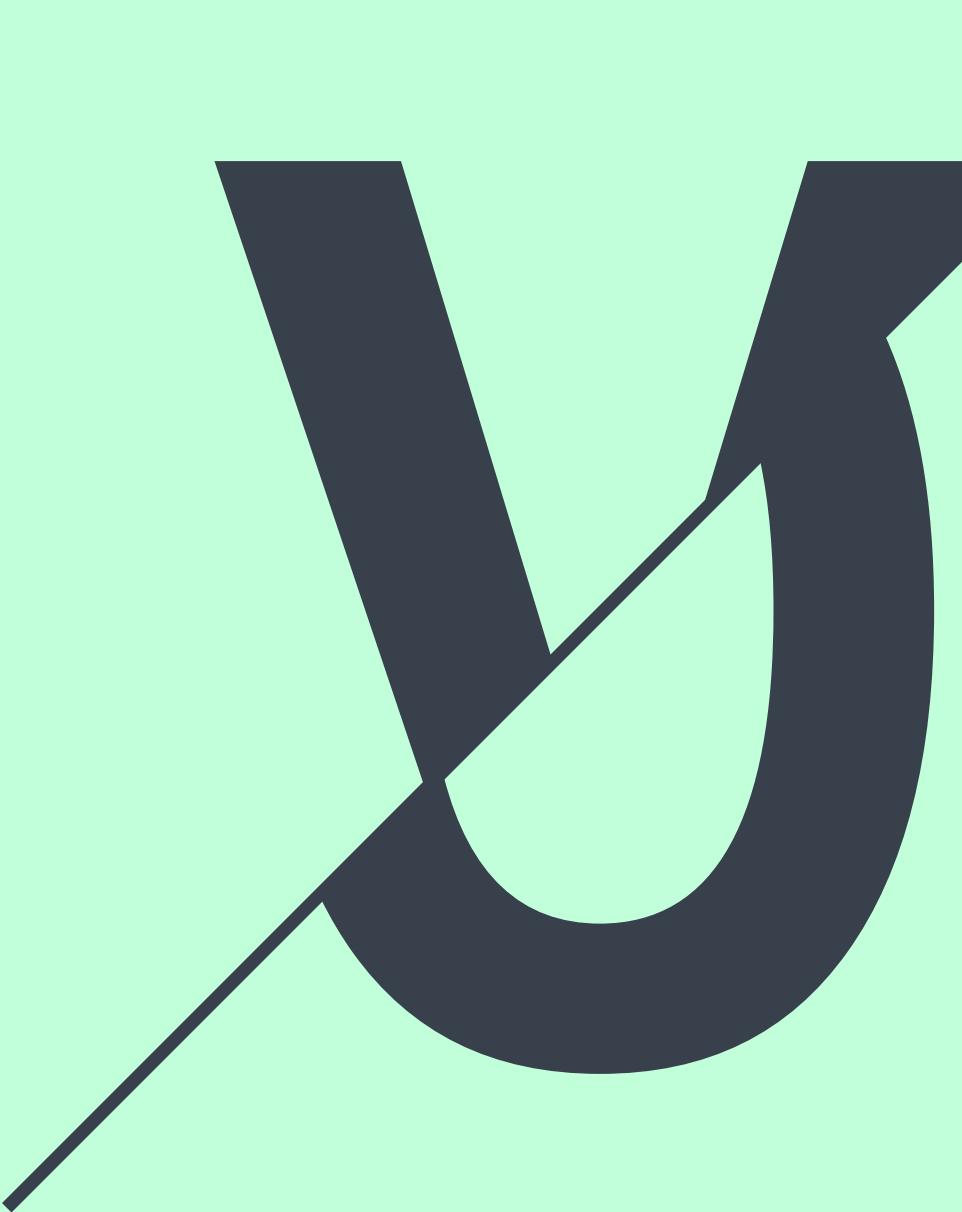
POTENTIAL THREATS

VERÄNDERUNG DERMACHTKONSTELLATIONEN





VIRTUAL WARFARE DAS VIRTUELLE SCHLACHTFELD



REAL IMPACTS



CURRENT ATTACKS



POTENTIAL THREATS





VIRTUAL WARFARE

DAS VIRTUELLE SCHLACHTFELD





WAS IST CYBERWAR?

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.





Dagegen gehen von zivilen Cyberattacken zumeist deutlich geringere Bedrohungen aus. Sie können nach Angreifer-Typ und Angriffsziel unterschieden werden. Da gibt es den »Teenager-hacker«, 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.

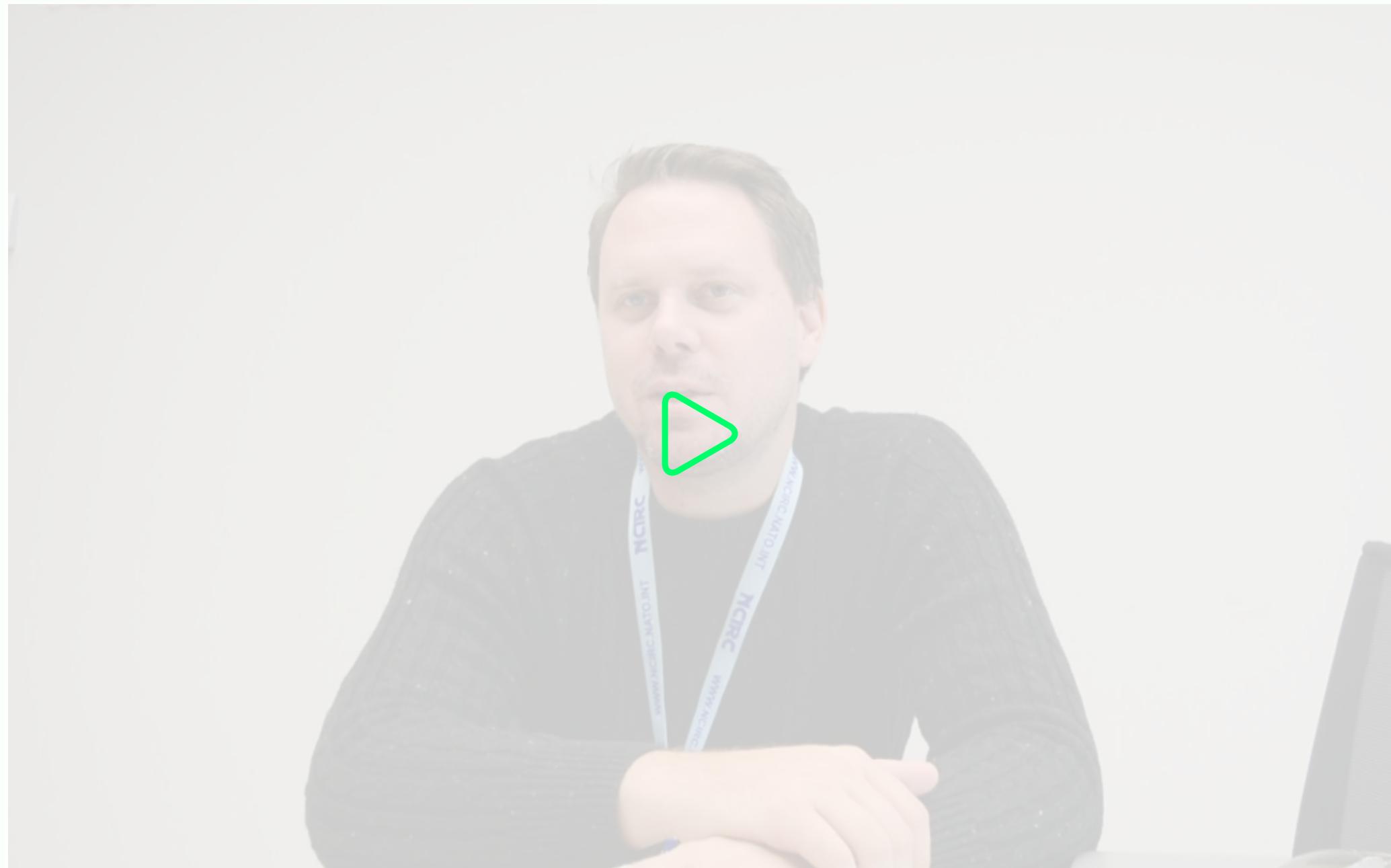




INTERVIEW MIT SANDRO GAYCKEN

2015 | 29. SEPTEMBER

Sandro Gaycken, der IT-Security Experte aus Berlin, erläutert Cyberwar im Gespräch mit dem »Zeroday« Team.





VIRTUAL WARFARE

ZERO DAY





WAS MEINEN DIE EXPERTEN?

Die Definition von Cyberwar ist unter den IT- und Sicherheits-experten genauso umstritten wie die Einschätzung der aktuellen und zukünftigen Bedrohung.

Klicke auf die Experten und erfahre mehr.



WAS MEINEN DIE EXPERTEN?

Die Definition von Cyberwar ist unter den IT- und Sicherheits-experten genauso umstritten wie die Einschätzung der aktuellen und zukünftigen Bedrohung.

Klicke auf die Experten und erfahre mehr.



P.W. Singer
Politikwissenschaftler

»Whether it be war on land, at sea, or in the air, or now in cyberspace, war always has a political goal
... (nicht militärische Ziele)«



P.W. Singer

Politikwissenschaftler

»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

»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

»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.«

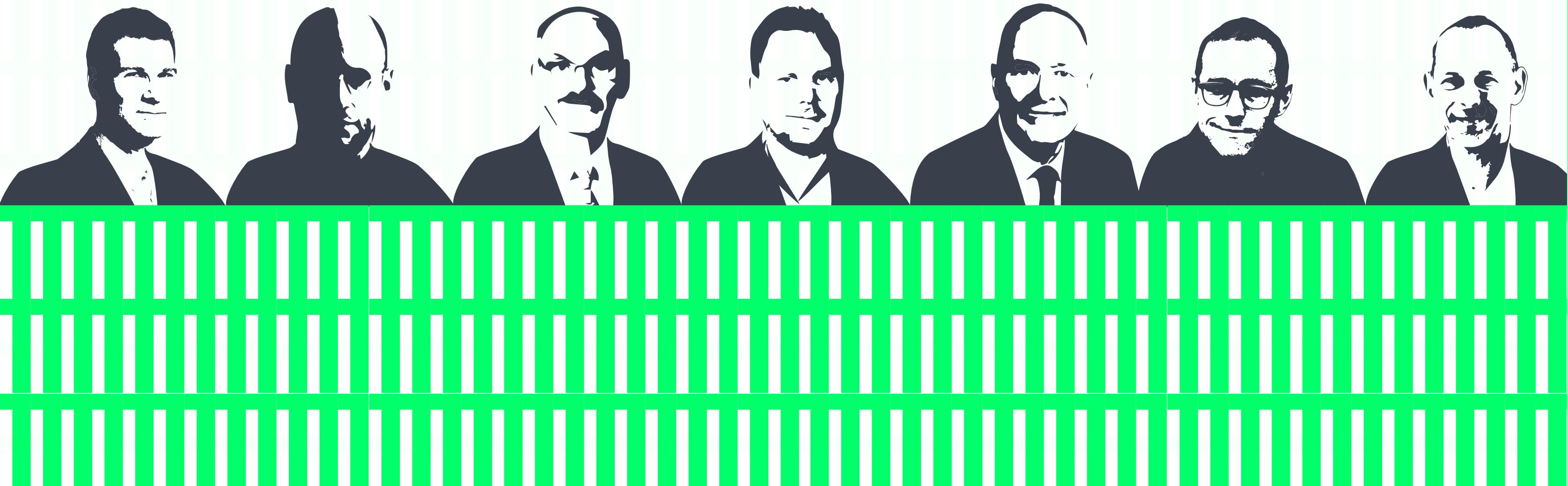




Malte Herwig
Politikwissenschaftler

»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.«





WAS ÄNDERT SICH AN DER KRIEGSFÜHRUNG?

WAS ÄNDERT SICH AN DER KRIEGSFÜHRUNG?

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

Christian Bartlau 2014

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



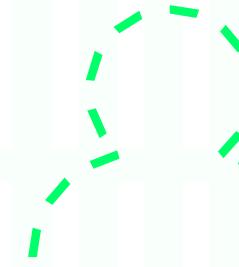
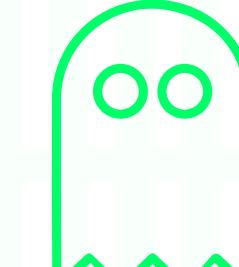


DER KRIEG DER ZUKUNFT

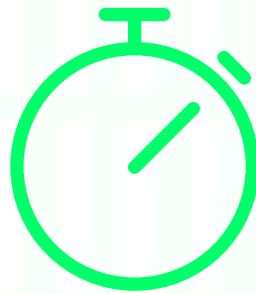
Christina Brinkmann

Cyberkrieg unterscheidet sich wesentlich von konventioneller Kriegsführung. Er verändert die Bedingungen für Angreifer wie für Abwehr. Er ist schneller.

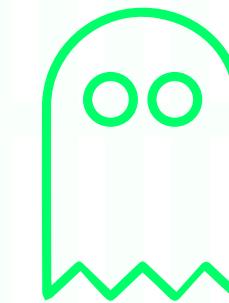
CHARAKTERISTIKA DER NEUEN KRIEGSFÜHRUNG



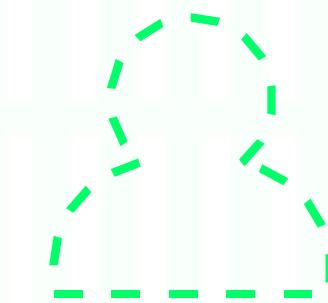
CHARAKTERISTIKA DER NEUEN KRIEGSFÜHRUNG



KRIEG OHNE
RAUM UND ZEIT



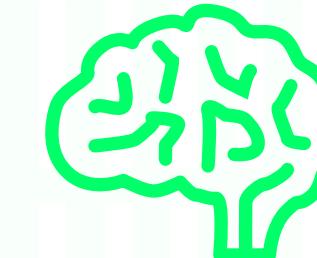
UNSICHTBARE
ANGRIFFE



ATTRIBUTIONS-
PROBLEM



GERINGES RISIKO
KLEINES GELD



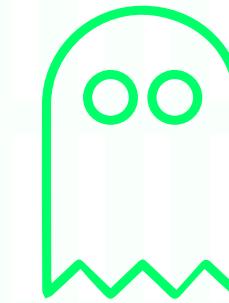
HOHE HACKER-
KOMPETENZ



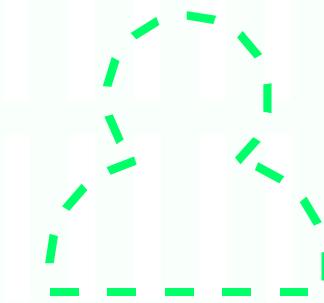
CHARAKTERISTIKA DER NEUEN KRIEGSFÜHRUNG



KRIEG OHNE
RAUM UND ZEIT



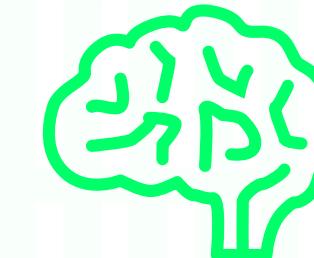
UNSICHTBARE
ANGRIFFE



ATTRIBUTIONS-
PROBLEM



GERINGES RISIKO
KLEINES GELD

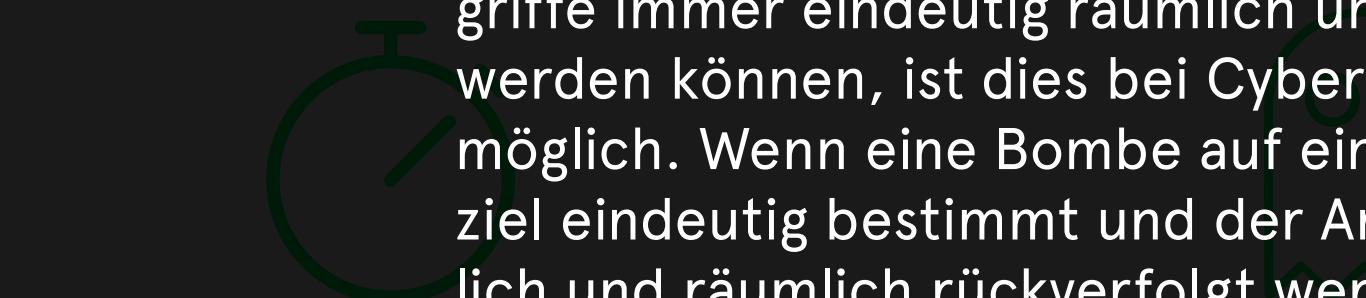


HOHE HACKER-
KOMPETENZ





DER KRIEG OHNE RAUM UND ZEIT



Das neue an Cyberwarangriffen 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 zumeist zeitlich und räumlich rückverfolgt werden.



KRIEG OHNE
RAUM UND ZEIT

UNSICHTBARE
ANGRIFFE

ATTRIBUTATIONS-
PROBLEM



Dies ist bei Cyberwar-Attacken nicht immer so. Ein Vierenangriff 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 Leichtgeschwindigkeit 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 Zielsystem steuert. So kann z.B. ein Angriff auf die Zentrale der deutschen Hochspannungsnetze in Hamburg dafür sorgen, dass in München die Stromversorgung ausfällt.

GERINGES RISIKO
KEINES GELD

HOHE HACKER-
KOMPETENZ





WAS MEINEN DIE EXPERTEN? JEN KRIEGSFÜHRUNG

Klicke auf die Experten und erfahre mehr.



KRIEG OHNE
RAUM UND ZEIT



UNSICHTBARE
ANGRIFFE



ATTRIBUTIONS-
PROBLEM





WAS MEINEN DIE EXPERTEN? JEN KRIEGSFÜHRUNG

Klicke auf die Experten und erfahre mehr.



KRIEG OHNE
RAUHEND ZEIT



Malte Herwig
Politikwissenschaftler



UNSICHTBARE
ANGRIFFE



ATTRIBUTIONS-
PROBLEM



»Whether it be war on land, at sea, or in the air, or now in cyberspace, war always has a political goal
... and (in the last analysis) a political solution.«

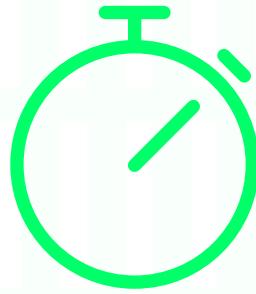


Malte Herwig
Politikwissenschaftler

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. [...]«



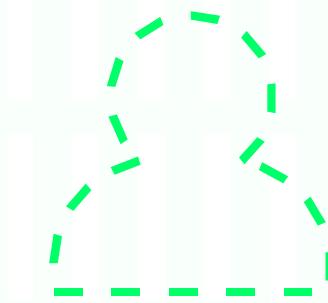
CHARAKTERISTIKA DER NEUEN KRIEGSFÜHRUNG



KRIEG OHNE
RAUM UND ZEIT



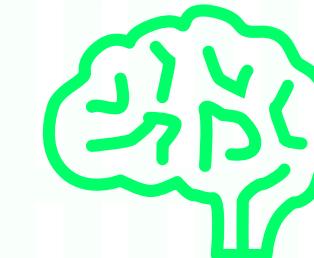
UNSICHTBARE
ANGRIFFE



ATTRIBUTIONS-
PROBLEM



GERINGES RISIKO
KLEINES GELD



HOHE HACKER-
KOMPETENZ





UNSICHTBARE ANGRIFFE NEUEN KRIEGSFÜHRUNG

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-Überwachungssystem oder die physikalischen Überwachungssysteme der Zielsysteme. So wird selbst die physische Zerstörung des Zielsystems erst bemerkt, wenn keine Gegenmaßnahmen mehr möglich sind.

Noch raffinierter 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.

KRIEG OHNE
RAUM UND ZEIT
UNSICHTBARE
ANGRIFFE
ATTRIBUTION-
PROBLEM





UNSICHTBARE ANGRIFFE NEUEN KRIEGSFÜHRUNG

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-Überwachungssystem oder die physikalischen Überwachungssysteme der Zielsysteme. So wird selbst die physische Zerstörung des Zielsystems erst bemerkt, wenn keine Gegenmaßnahmen mehr möglich sind.

Noch raffinierter 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.



ATTRIBUTION-
PROBLEM



»Cyberwar – Das Wettrüsten hat längst begonnen«
Sandro Gaycken





WAS MEINEN DIE EXPERTEN? JEN KRIEGSFÜHRUNG

Klicke auf die Experten und erfahre mehr.



KRIEG OHNE
RAUHEND ZEIT



Malte Herwig
Politikwissenschaftler



UNSICHTBARE
ANGRIFFE



ATTRIBUTIONS-
PROBLEM



»Whether it be war on land, at sea, or in the air, or now in cyberspace, war always has a political goal
... and (in the last analysis) a political purpose.«

X



INTERVIEW MIT PETER W. SINGER

How Drones are Like Viruses (and Vice-Versa)

Peter W. Singer
Political Scientist

0:05 / 3:50

big think

Subscribe to Big Think Mentor.

Subscribe to Big Think Edge.

Subscribe to Big Think.

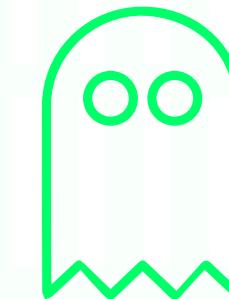
big think

HD YouTube

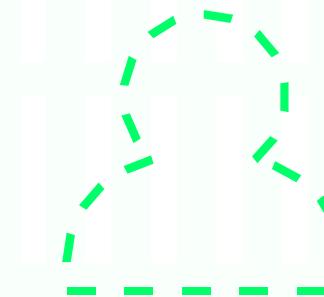
↑



KRIEG OHNE
RAUM UND ZEIT



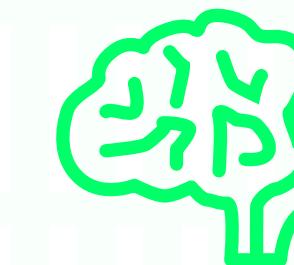
UNSICHTBARE
ANGRIFFE



ATTRIBUTIONS-
PROBLEM



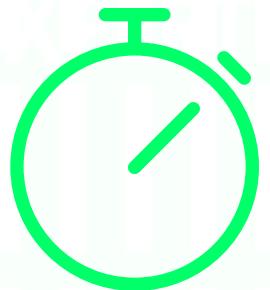
GERINGES RISIKO
KLEINES GELD



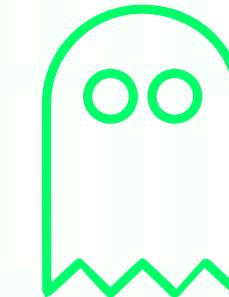
HOHE HACKER-
KOMPETENZ



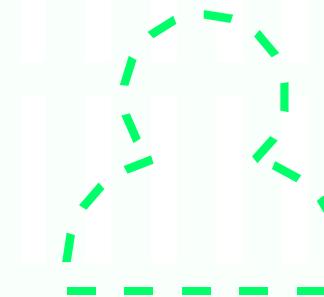
REAL IMPACTS



KRIEG OHNE
RAUM UND ZEIT



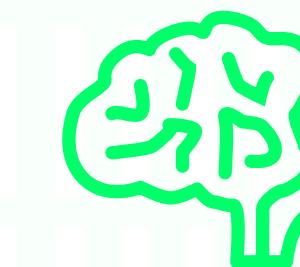
UNSICHTBARE
ANGRIFFE



ATTRIBUTATIONS-
PROBLEM



GERINGES RISIKO
KLEINES GELD



HOHE HACKER-
KOMPETENZ

REAL IMPACTS



REAL IMPACTS
AUSWIRKUNGEN AUF DIE REALE WELT

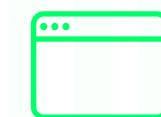


VIRTUALISIERUNG DER WELT

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

Marcel Kolenbach 2013

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 großen Zerstörungen in der realen Welt führen.

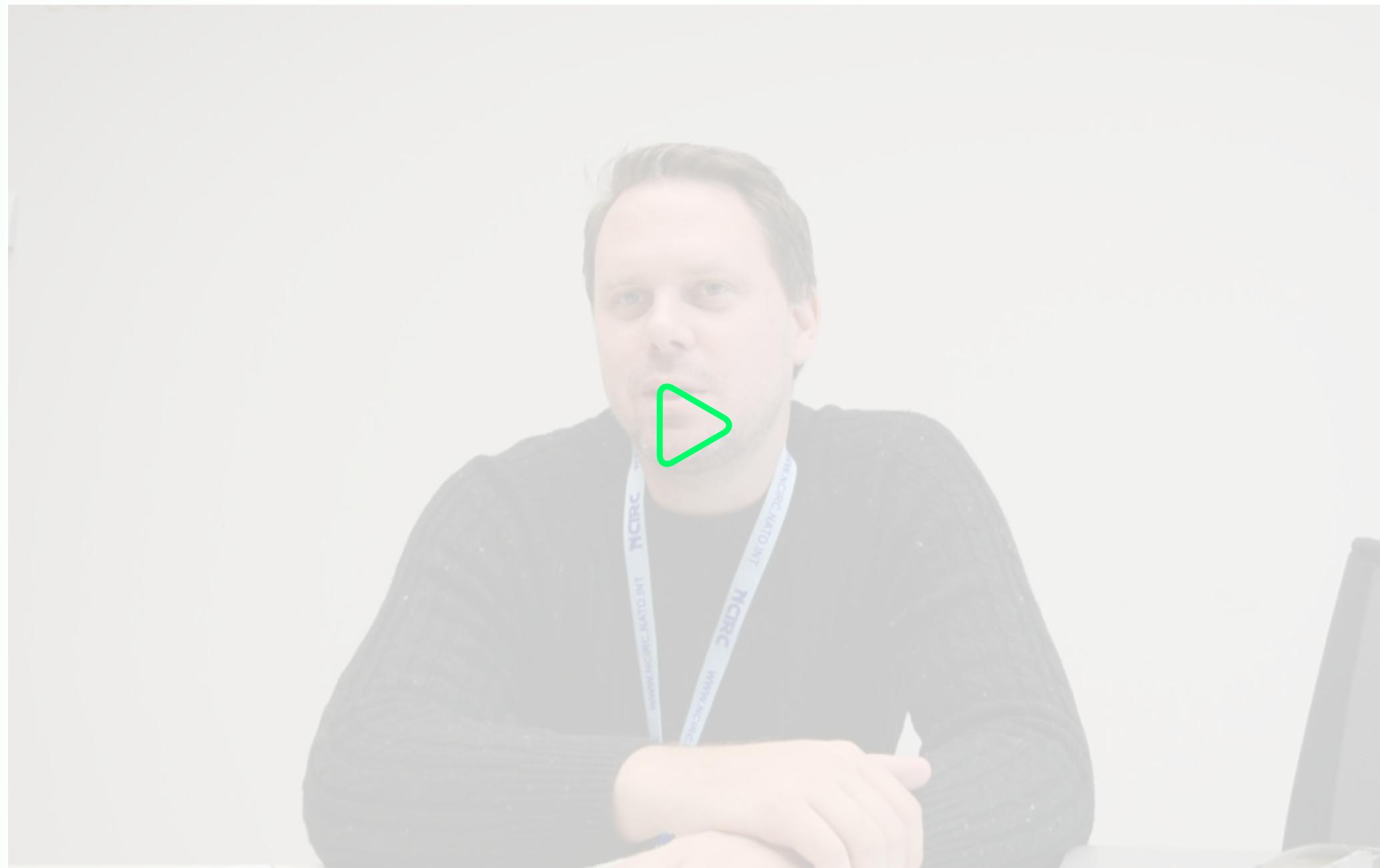




INTERVIEW MIT SANDRO GAYCKEN

2015 | 29. SEPTEMBER

Sandro Gaycken, der IT-Security Experte aus Berlin, erläutert Cyberwar im Gespräch mit dem »Zeroday« Team.





REAL IMPACTS

ZERO DAY



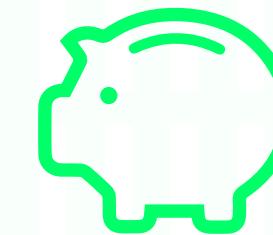
ABHÄNGIGKEIT VON VERNETZEN SYSTEMEN

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



INFORMATIONSMEDIEN

Was wir wissen, wissen wir von unseren Informationsmedien.



WIRTSCHAFT & FINANZMARKT

Wirtschaftliche Krisen können zur sozialen Not führen.

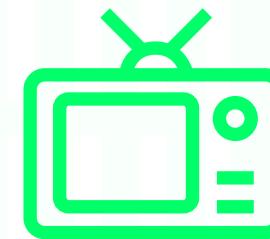


KRITSCHE INFRASTRUKTUR

Ohne Strom gehen nicht nur die Lichter aus.

ABHÄNGIGKEIT VON VERNETZEN SYSTEMEN

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



INFORMATIONSMEDIEN

Was wir wissen, wissen wir von unseren Informationsmedien.



WIRTSCHAFT & FINANZMARKT

Wirtschaftliche Krisen können zur sozialen Not führen.

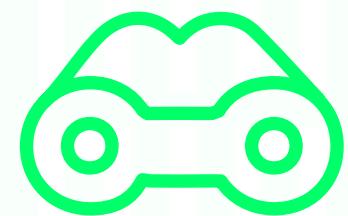


KRITSCHE INFRASTRUKTUR

Ohne Strom gehen nicht nur die Lichter aus.

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

Die NSA ist nur spitze des Eisbergs.



MANIPULATION

Wenn die eigenen technischen Systeme dem Gegner gehorchen.



SABOTAGE

Maschinen, die sich selbst zerstören.

**SPIONAGE**

Die NSA ist nur spitze
des Eisbergs.

**MANIPULATION**

Wenn die eigenen techni-
schen Systeme dem
Gegner gehorchen.

**SABOTAGE**

Maschinen, die sich
selbst zerstören.





SPIONAGE

Die NSA ist nur spitze
des Eisbergs.



MANIPULATION

Wenn die eigenen techni-
schen Systeme dem
Gegner gehorchen.



SABOTAGE

Maschinen, die sich
selbst zerstören.



CURRENT ATTACKS

DIE GESCHICHTE DER CYBERATTACKEN



DIE GESCHICHTE DER CYBERATTACKEN

Cyberwar als Krieg zwischen zwei Staaten konnte noch nicht beobachtet werden. Trotzdem werden in den Medien immer öfters Cyber-Attacken beschrieben, die zeigen, welchen Schaden solche Angriffe bewirken können. Im Gegensatz zu Cyberwar gehen solche Angriffe zumeist von nichtmilitärischen Akteuren aus. Doch aufgrund des Attributionsproblems ist es sehr schwer den tatsächlichen Angreifer zu identifizieren. Deshalb braucht es zumeist einige Zufälle um einem professionellen Angreifer auf die Spur zu kommen. So ist heute wohl klar, dass der Stuxnet Angriff auf die iranische Atomwirtschaft militärisch geplant und durchgeführt wurde.



» In jedem Fall war Stuxnet aber die erste echte Demonstration militärischer Macht im Cyberwar, ein erstes Indiz für die reale Gewalt des Cyberwar [...] Seit Stuxnet muss das Thema Cyberwar ernst genommen werden. «

Sandro Gaycken 2011

Auch Terrororganisationen wie der IS haben gezeigt, dass sie der Lage sind Cyberattacken anzuwenden. Beispielsweise blockierten IS-Hacker am 11. Januar 2015 die Internetseiten französischer Organisationen und am 8. April 2015 übernahm der IS die Kontrolle über den französischen Fernsehsender TV 5 Monde. Demgegenüber steht die Hackergruppe »Anonymous«, die den IS-Hackern den Krieg erklärt hat. Sowohl nach dem Anschlag auf das Satiremagazin »Charlie Hebdo« als auch nach den aktuellen Anschlägen in Paris haben Anonymous-Aktivisten die Twitter-Konten von mehreren Tausend IS-Sympathisanten blockiert. In der folgenden Timeline werden nun einige der bekanntgewordenen Fälle von Cyberangriffen dokumentiert.

2015	FEB
2014	MÄR
2013	APR
2012	DEZ
2011	
2010	
2009	
2008	
2007	
2006	
2005	
2004	
2003	
2002	
2001	
2000	
1999	
1998	
1982	

2015 | 7. APRIL 12:00 UHR

ALLJÄHLICHE HACKERATTACKE ISRAEL

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. >>

2015 | 8. APRIL 22:00 UHR

IS-HACKERATTACKE AUF TV5 MONDE FRANKREICH

Abends um 22 Uhr wird der Bildschirm von TV5 Monde schwarz: IS-Hacker haben sich ins Netzwerk des französisch-sprachigen Senders eingehackt und auch die Kontrolle über die Internet- und Facebook-Seite, sowie das Twitterkonto des

2015 FEB
2014 MÄR
2013 APR
2012 DEZ
2011
2010
2009
2008
2007
2006
2005
2004
2003
2002
2001
2000
1999
1998
1982

2015 | 7. APRIL 12:00 UHR
ALLJÄHLICHE HACKERATTACKE
ISRAEL

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. >>

2015 | 8. APRIL 22:00 UHR
IS-HACKERATTACKE AUF TV5 MONDE
FRANKREICH

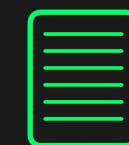
Abends um 22 Uhr wird der Bildschirm von TV5 Monde schwarz: IS-Hacker haben sich ins Netzwerk des französisch-sprachigen Senders eingehackt und auch die Kontrolle über die Internet- und Facebook-Seite, sowie das Twitterkonto des

2015
2014
2013
2012
2011
2010
2009
2008
2007
2006
2005
2004
2003
2002
2001
2000
1999
1998
1982

FEB 2015 | 7. APRIL 12:00 UHR
2015 | 7. APRIL 12:00 AM

ALLJÄHLICHE HACKERATTACKE ISRAEL

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. 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.



2015

FEB

2015 | 7. APRIL 12:00 UHR

2014

MÄR

DOKUMENTATION HE HACKERATTACKE

2013

APR

ISRAEL

2012

DEZ

2015 | 22. OKTOBER

2011

Der Spiegel berichtet in einer Dokumentation über die Hacker-
attacke auf Israel.

Seit 2013 ist der 7. April Tag der Cyberangriffe. In diesem Jahr

2010

wurden offenbar mehrere israelische Webseiten angegriffen,
darunter zahlreiche Seiten der Regierung. Hinter den Angriffen

2009

2008

2007

2006

2005

2004

2003

2002

2001

2000

1999

1998

1982





1982

PIPELINE-EXPLOSION

SOWJETUNION

2013

2012

2011

2010

2009

2008

2007

2006

2005

2004

2003

2002

2001

2000

1999

1998

1982

Russland versuchte, an US-Hochtechnologiesysteme zur Steuerung der eigenen Pipelines zu gelangen, die ihnen die USA wegen des kalten Krieges nicht überlassen wollten. Die USA ließen die Entwendungen dennoch zu, bauten aber in die Software ein Schadprogramm ein, durch das 1982 der Druck in der Tscheljabinsk-Pipeline über den zulässigen Höchstwert gebracht wurde. Es folgte eine Explosion von ca. 3 Kilotonnen Stärke, immerhin einem Fünftel der Hiroshima-Bombe. Russland widersprach dieser Darstellung der Ereignisse. >>>



2013

2012

2011

2010

2009

2008

2007

2006

2005

2004

2003

2002

2001

2000

1999

1998

1982

PIPELINE-EXPLOSION

SOWJETUNION

Russland versuchte, an US-Hochtechnologiesysteme zur Steuerung der eigenen Pipelines zu gelangen, die ihnen die USA wegen des kalten Krieges nicht überlassen wollten. Die USA ließen die Entwendungen dennoch zu, bauten aber in die Software ein Schadprogramm ein, durch das 1982 der Druck in der Tscheljabinsk-Pipeline über den zulässigen Höchstwert gebracht wurde. Es folgte eine Explosion von ca. 3 Kilotonnen Stärke, immerhin einem Fünftel der Hiroshima-Bombe. Russland widersprach dieser Darstellung der Ereignisse. >>>



POTENTIAL THREATS

VERÄNDERUNG DERMACHTKONSTELLATIONEN



VERÄNDERUNG DER WELTWEITEN MACHTKONSTELLATION

Cyberwar als andere Art der Kriegsführung schafft sowohl neue Angriffsmöglichkeiten als auch neue Angriffsflächen der Länder. Dies wird zukünftige Kriege verändern. Aber noch haben wir keinen Cyberwar zwischen Staaten erlebt. Die bisher dokumentierten Cyberangriffe zeigen aber, welche Potentiale und Gefahren sich aus diesen neuen Angriffsmethoden ergeben können. Die Militärs aus aller Welt bereiten sich mit hohem finanziellem und personellem Einsatz auf diese Veränderung der Gefährdungslage vor. Diese geschieht aufgrund militärischer Geheimhaltung weitgehend unter Ausschluss der Öffentlichkeit. Experten schätzen aber, dass insbesondere die USA, China und Russland aber auch militärisch bisher eher schwache Länder wie Nordkorea zu den aktivsten Cyberwar-Akteuren zählen. Auch die Bundeswehr hat jetzt ihre Aktivitäten zu diesem Thema ausgebaut.



DEFINITION ANTI-ASYMMETRIE

Unter den Bedingungen der konventionellen Kriegsführung war die militärische Aufrüstung die wichtigste Voraussetzung für die Fähigkeit von Staaten Krieg zu führen und zu gewinnen. Gleichzeitig bot diese Fähigkeit auch den größten Schutz vor militärischen Angriffen, da ein möglicher Aggressor mit vernichtenden Gegenschlägen rechnen musste. Dieses Verhältnis hat zu Zeiten des Kalten Krieges zur Anhäufung von atomaren Massenvernichtungswaffen bei wenigen mächtigen Staaten geführt. Da solche Waffenarsenale nur mit höchstem finanziellem Aufwand zu beschaffen sind, waren gerade wirtschaftlich starke Staaten zumeist auch die militärisch mächtigsten Staaten. Die wirtschaftlichen Asymmetrien in der Welt wurden dadurch militärisch noch verstärkt.

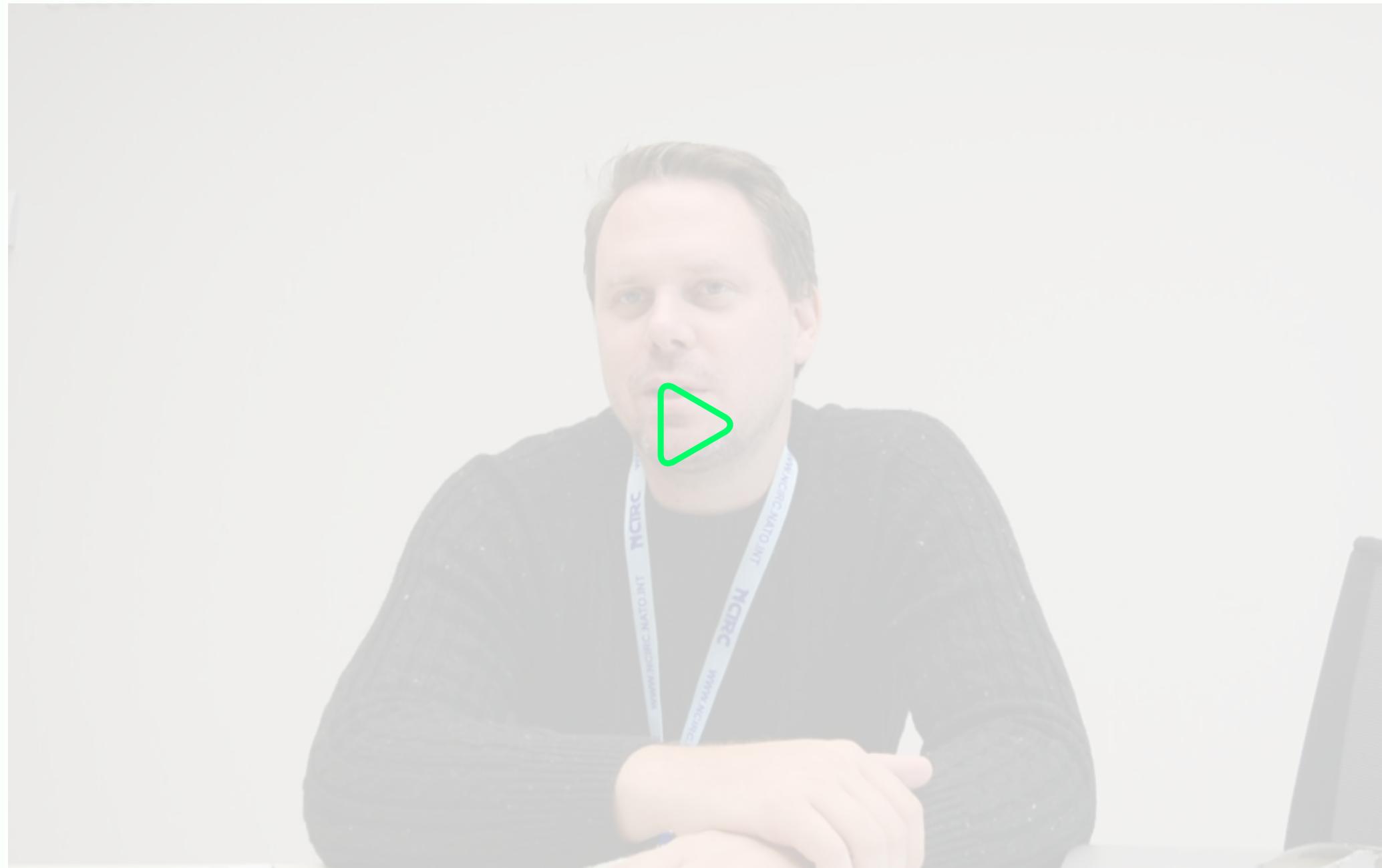


Cyberwar könnte diese Verhältnisse in Zukunft grundlegend ändern. Die Cyberangriffsfähigkeit kann mit geringem finanziellem Aufwand hergestellt werden. Aufgrund des Attributionsproblems verlieren potentielle Gegenschläge ihre abschreckende Wirkung. Auf der anderen Seite sind daher gerade Staaten besonders gefährdet, die sich stark von IT-Vernetzungen abhängig gemacht haben. Dies trifft vorwiegend auf die wirtschaftlich starken Staaten zu.

INTERVIEW MIT SANDRO GAYCKEN

2015 | 29. SEPTEMBER

Sandro Gaycken, der IT-Security Experte aus Berlin, erläutert Cyberwar im Gespräch mit dem »Zeroday« Team.





POTENTIAL THREATS

ZERO DAY



INTERACTIVE MAP – WIE FUNKTIONIERTS?

Ziel der »Interactive Map« ist es die unterschiedlichen Gefährdungslagen durch konventionelle Kriegsführung und durch Cyberwar der einzelnen Staaten zu visualisieren. Damit werden die Veränderungen vom »Coldwar« zum »Codewar« sichtbar und der Begriff der »Anti-Asymmetrien« auf der Grundlage realer statistischer Daten visualisiert.

Auf der dargestellten Weltkarte werden die Indizes für die Gefährdung durch Cyberwar (»Codewar Threat«) und für die Gefährdung durch konventionelle Kriegsführung (»Conventional Threat«) dargestellt. Somit wird für jedes Land aufgezeigt in wie weit die neuen Kriegsführungsmöglichkeiten ihre Gefährdungslage vergrößern oder verkleinern. Dabei werden einige überraschende Effekte deutlich. Durch die Darstellung des jeweiligen Bruttoinlandsprodukts (BIP) können die unterschiedlichen Veränderungen der Gefährdungslagen mit der Wirtschaftskraft des jeweiligen Landes korreliert werden.

LOS GEHTS!



INTERACTIVE MAP – WIE FUNKTIONIERTS?

Ziel der »Interactive Map« ist es die unterschiedlichen Gefährdungslagen durch konventionelle Kriegsführung und durch Cyberwar der einzelnen Staaten zu visualisieren. Damit werden die Veränderungen vom »Coldwar« zum »Codewar« sichtbar und der Begriff der »Anti-Asymmetrien« auf der Grundlage realer statistischer Daten visualisiert.

Auf der dargestellten Weltkarte werden die Indizes für die Gefährdung durch Cyberwar (»Codewar Threat«) und für die Gefährdung durch konventionelle Kriegsführung (»Conventional Threat«) dargestellt. Somit wird für jedes Land aufgezeigt in wie weit die neuen Kriegsführungsmöglichkeiten ihre Gefährdungslage vergrößern oder verkleinern. Dabei werden einige überraschende Effekte deutlich. Durch die Darstellung des jeweiligen Bruttoinlandsprodukts (BIP) können die unterschiedlichen Veränderungen der Gefährdungslagen mit der Wirtschaftskraft des jeweiligen Landes korreliert werden.

LOS GEHTS!





POTENTIAL THREATS

ZERO DAY



INFO

CODEWAR THREAT

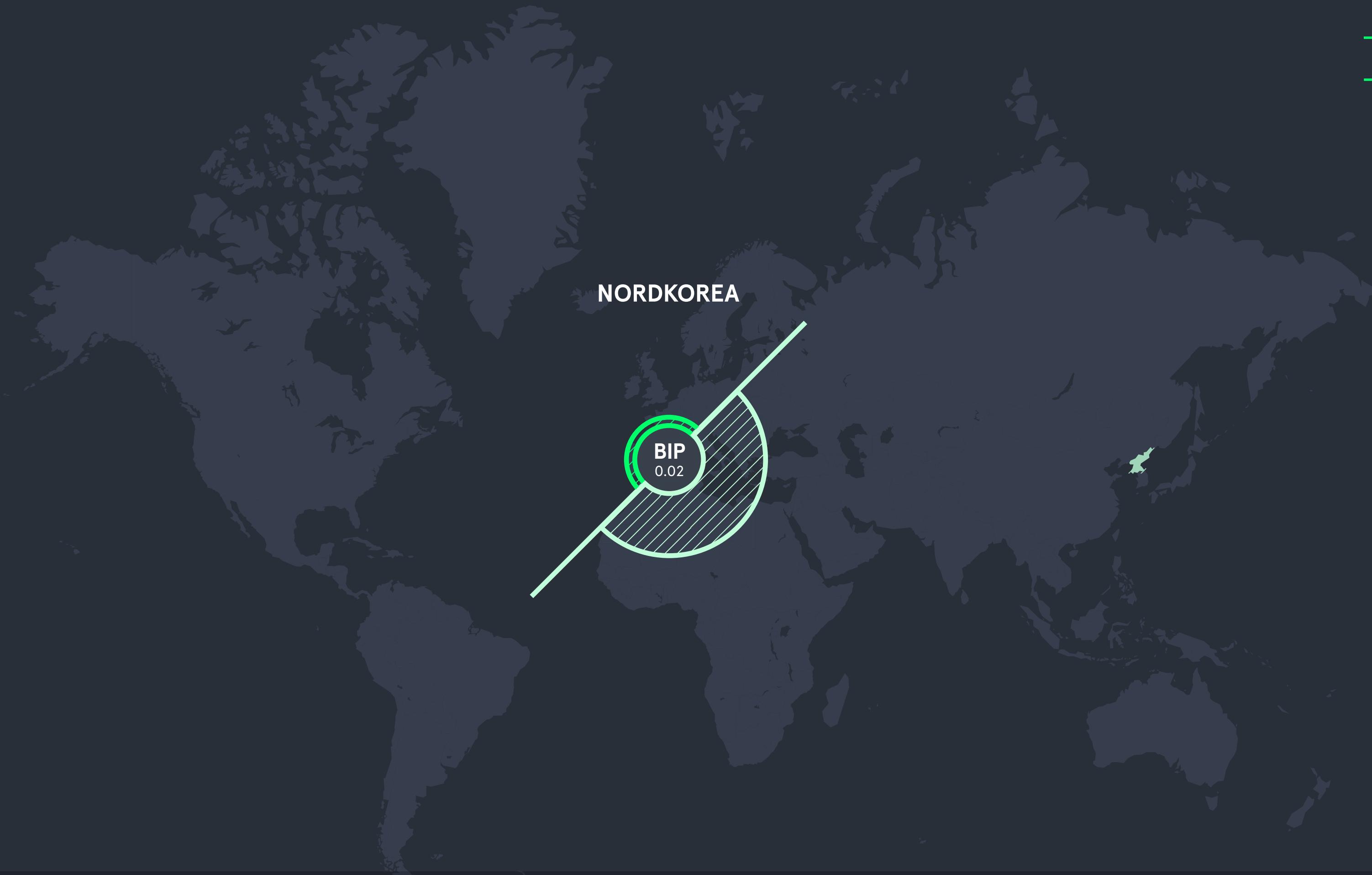
CONVENTIONAL THREAT

BIP













RUSSLAND

BIP

16.8

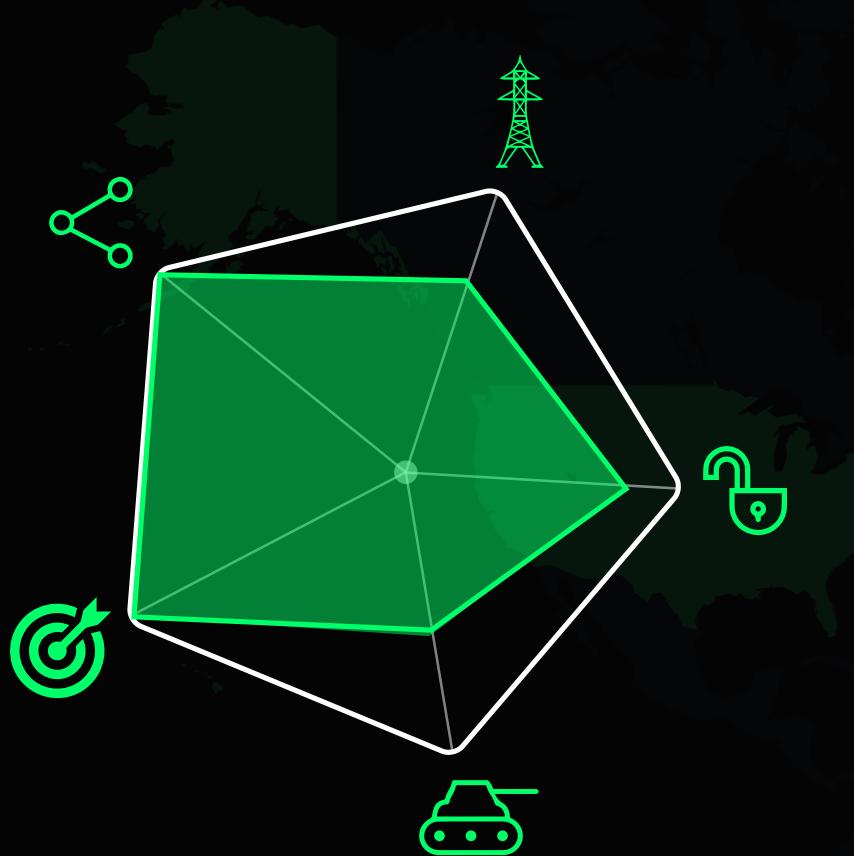




VEREINIGTE STAATEN

BIP
16.8

VEREINIGTE STAATEN



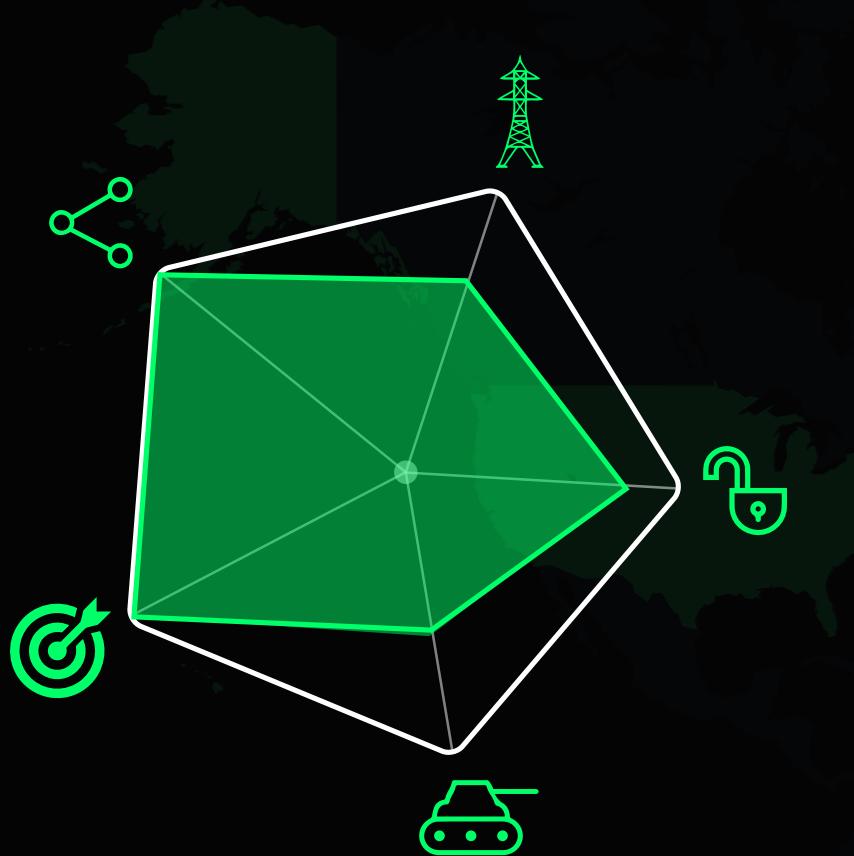
	NETWORKING	10.0	
	5.008 IP-ADRESSEN PRO 1.000 EINWOHNER		
	INFRASTRUCTURE	7.2	
	12.186 KWH PRO EINWOHNER		
	OPEN NET	8.1	
	8.1 DEMOKRATIEINDEX		
	CONFLICTS	6.3	
	7 KRIEGSKONFLIKTE		CONFLICTS
	CYBERATTACKS	10.0	
	256.659 CYBERAN- GRIFFE PRO TAG		7 KRIEGSKONFLIKTE



Der Flächeninhalt der Pentagon-Grafik visualisiert den »Codewar Threat« Index.



VEREINIGTE STAATEN



	NETWORKING	10.0	
	5.008 IP-ADRESSEN PRO 1.000 EINWOHNER		
	INFRASTRUCTURE	7.2	
	12.186 KWH PRO EINWOHNER		
	OPEN NET	8.1	
	8.1 DEMOKRATIEINDEX		
	CONFLICTS	6.3	
	7 KRIEGSKONFLIKTE		CONFLICTS
	CYBERATTACKS	10.0	
	256.659 CYBERAN- GRIFFE PRO TAG		7 KRIEGSKONFLIKTE



Der Flächeninhalt der Pentagon-Grafik visualisiert den »Codewar Threat« Index.



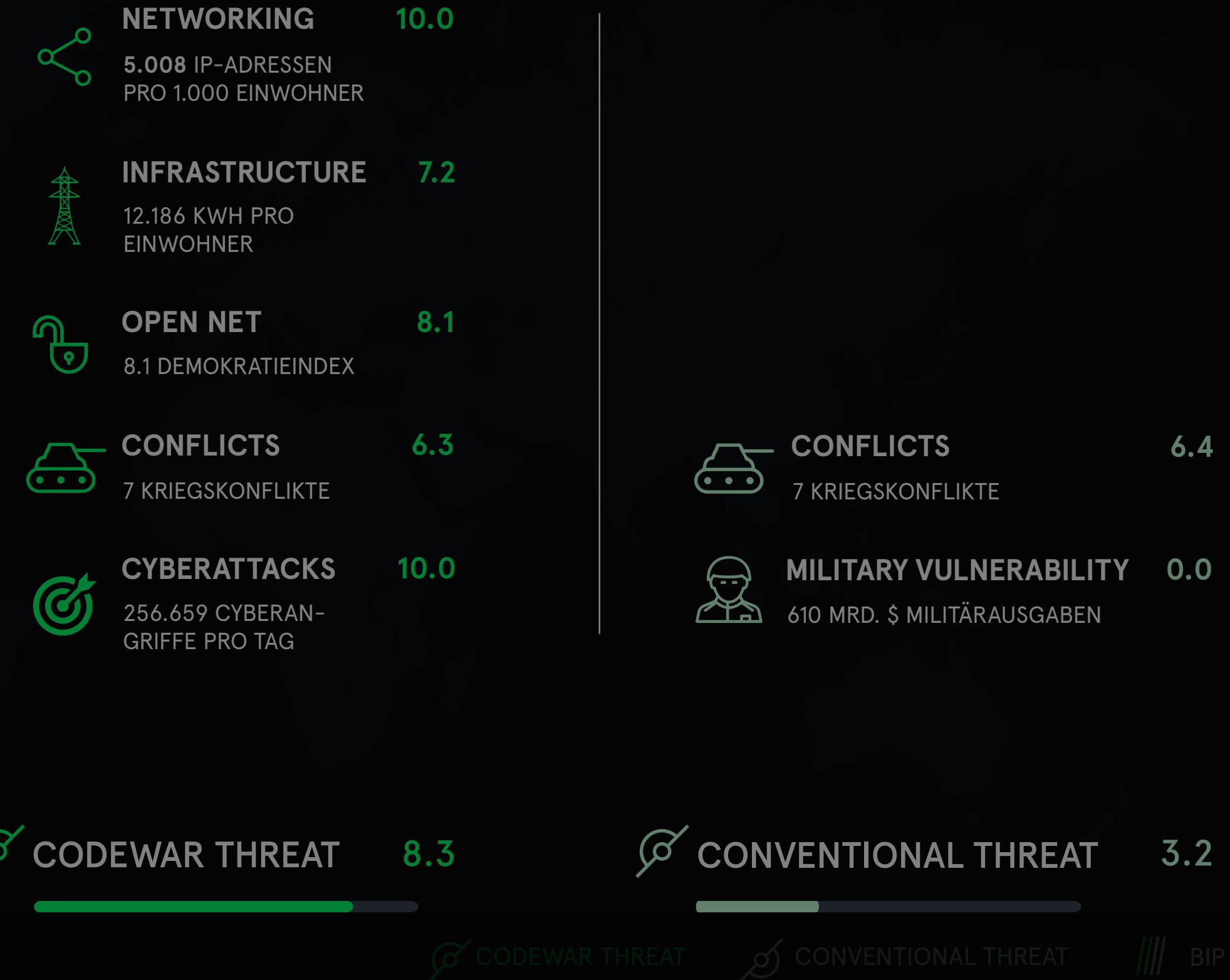


GEFÄHRDUNGSFAKTOREN

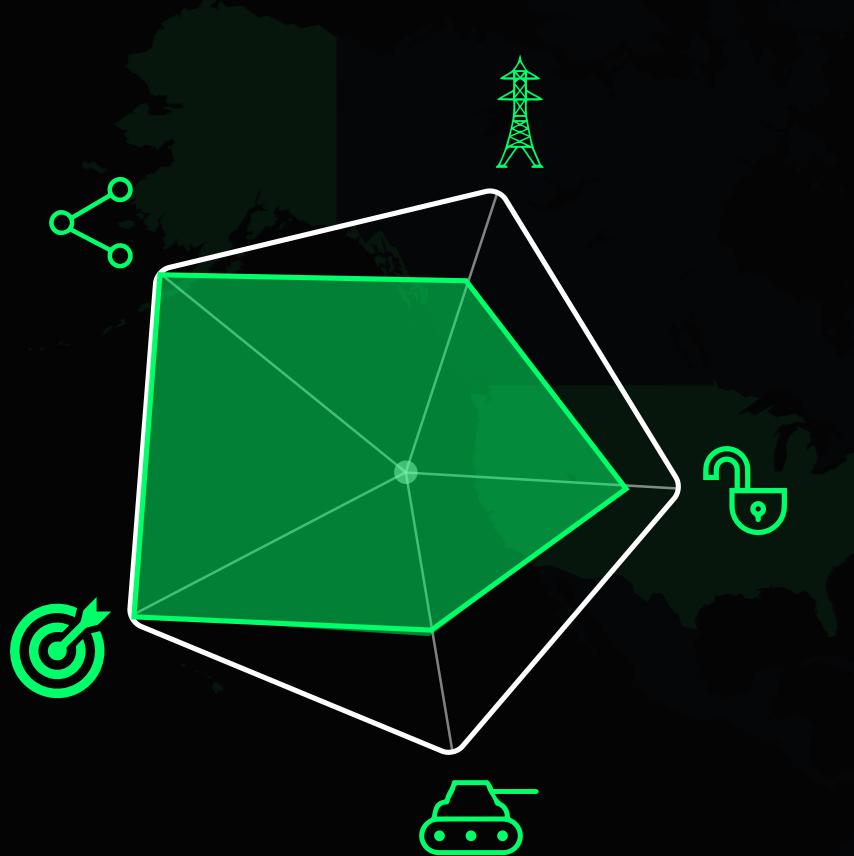
Die einzelnen Gefährdungsfaktoren werden mit einem Icon und dem berechneten Indexwert 0-10 dargestellt.

Der Mittelwert der Gefährdungsfaktoren ergibt den »Threat« Index 0-10. Dieser wird im »Codewar Threat« und »Conventional Threat« Barometer dargestellt.

Der »Codeware Threat« Index wird in der Pentagon-Grafik als Fläche visualisiert.



VEREINIGTE STAATEN



	NETWORKING	10.0	
	5.008 IP-ADRESSEN PRO 1.000 EINWOHNER		
	INFRASTRUCTURE	7.2	
	12.186 KWH PRO EINWOHNER		
	OPEN NET	8.1	
	8.1 DEMOKRATIEINDEX		
	CONFLICTS	6.3	
	7 KRIEGSKONFLIKTE		CONFLICTS
	CYBERATTACKS	10.0	
	256.659 CYBERAN- GRIFFE PRO TAG		7 KRIEGSKONFLIKTE



Der Flächeninhalt der Pentagon-Grafik visualisiert den »Codewar Threat« Index.





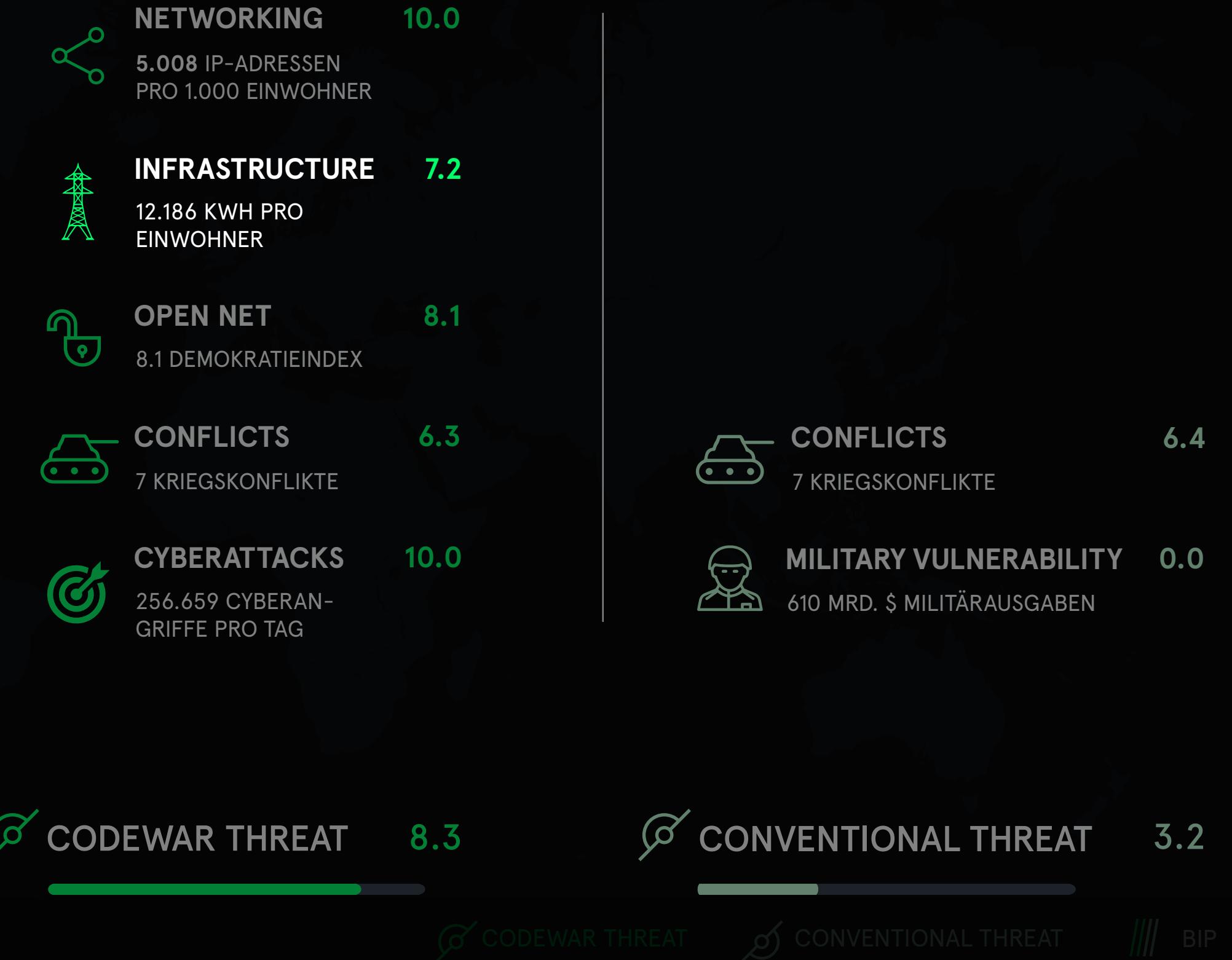
INFRASTRUCTURE

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.

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

Indikator:
Kilowattstunden pro Einwohner

Quelle:
Für 2014, CIA-World-Factbook²





MILITARY VULNERABILITY

In der konventionellen Kriegsführung war ist die militärische Aufrüstung der größte Schutz vor Angriffen, da ein möglicher Aggressor mit vernichtenden Gegenschlägen rechnen muss. Als Messindikator für die militärische Konfliktfähigkeit werden die Militärausgaben eines Landes herangezogen.

Je höher der Militärhaushalt, desto stärker das Militär, desto geringer die Gefahr konventioneller Kriege. Damit wird der Index »Military Vulnerability« aus dem Kehrwert des Indikators Militärausgaben berechnet.

Indikator:
MRD. \$ Militärausgaben

Quelle:
Militärausgaben für 2014 laut Friedensforschungsinstitut SIPRI⁷

