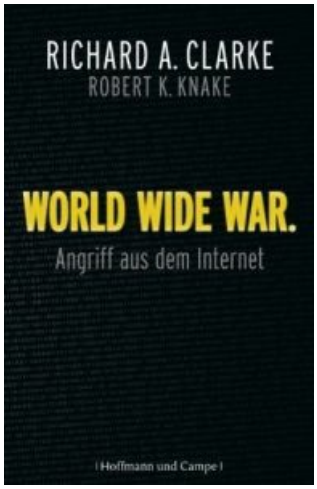

Buch World Wide War

Angriff aus dem Internet

Richard A. Clarke und Robert K. Knake
Hoffmann und Campe, 2011
Listen now

- play
- pause

00:00
00:00

Rezension

Was im Film *War Games* noch unter Science-Fiction lief, ist längst beängstigende Wirklichkeit geworden. Mussten bislang Soldaten oder Terroristen in fremde Länder eindringen, um Katastrophen auszulösen, genügt es heute, vom Schreibtisch aus ein paar schädliche Programmcodes bei Stromversorgern, Chemiefabriken oder Verkehrsunternehmen einzuschleusen. Das reicht, um in null Komma nichts ein ganzes Land aus den Angeln zu heben. Sicherheitsexperte Richard A. Clarke zeichnet, basierend auf seinen Erfahrungen als US-Bundeskoordinator für nationale Sicherheit, gemeinsam mit seinem Autorenkollegen ein düsteres Bild von den Möglichkeiten der Kriegsführung im Internet. Wie weit Staaten wie China, Nordkorea und Russland heute bereits gehen, dürfte die meisten Leser ängstigen. Tröstend ist, dass es offenbar Wege gibt, den Einsatz von Cyberwaffen immerhin zu beschränken. Das exzellent geschriebene und hochspannende Buch wirft die Frage auf, ob eine totale Vernetzung aller Lebensbereiche wirklich sinnvoll ist. *BooksInShort* empfiehlt es allen, die wissen wollen, welche Gefahren im Internet drohen.

Take-aways

- Krieg wird heute nicht mehr nur mit Waffen geführt, sondern auch übers Internet.
- Cyberangriffe erfolgen extrem schnell und weltweit. Sie beschränken sich keineswegs nur auf militärische Ziele.
- Circa 20–30 Staaten haben sich bereits für den Netzkrieg gerüstet.
- Angriffe über das Internet sind über zahlreiche Schwachstellen möglich, z. B. wegen unzureichender Datenverschlüsselung.
- Die USA haben eine starke Offensivkraft im Cyberkrieg, hinsichtlich der Defensive gibt es jedoch noch viel zu tun.
- Während in den USA der Privatsektor bei der Cybersicherheit ganz auf sich allein gestellt ist, unterliegt in China alles der staatlichen Kontrolle.
- Die USA benötigt eine defensive Triade: Schutz des Basisnetzes, des Stromnetzes und des Verteidigungsministeriums.
- Idealerweise sollten Stromkonzerne vom Internet abgekoppelt sein.
- Beim Cyberkrieg ist der Erstangreifer im Vorteil, da der anderen Seite u. U. noch die passende Abwehr fehlt.
- Wie für die Atomwaffen wäre auch für den Cyberkrieg ein beschränkender Vertrag nötig.

Zusammenfassung

Weltweite Angriffe in Lichtgeschwindigkeit

Krieg wird heute nicht mehr nur mit Bomben, Rakten und anderen Waffen geführt, sondern auch mit Software im Internet und in sonstigen Computernetzwerken. Ein bekanntes Beispiel ist der Virus Stuxnet, der 2010 weltweit industrielle Steuersysteme zum Erliegen brachte. Er zielte auf die Siemens-Software WinCC-S7 ab, die zur Steuerung und Überwachung von Maschinen eingesetzt wird. Im konkreten Fall waren die Angreifer besonders an den Urananreicherungsanlagen im Iran interessiert.

Übergriffe aus dem Cyberspace, wie der virtuelle Raum auch genannt wird, gab es aber schon wesentlich früher. So soll die israelische Luftwaffe im Jahr 2007 Syriens nagelneues Luftabwehrsystem gehackt haben, um eine angebliche nordkoreanische Atomwaffenfabrik im Osten des Landes bombardieren zu können. In diesem Fall soll der Feind mittels Radar in die Datennetze eingedrungen sein. Möglich ist allerdings auch, dass Agenten das Computersystem mit einem Trojaner, einem feindlichen Programmcode, infiziert und manipuliert haben; oder aber dass ein israelischer Agent ein Glasfaserkabel des Luftabwehrsystems geöffnet und darüber ein feindliches Softwarepaket eingeschleust hat.

> „Angriffe im virtuellen Raum nehmen in jedem Konflikt rasch globale Ausmaße an, da insgeheim gekaperte oder gehackte Computer und Server in aller Welt dafür genutzt werden."

Nachdem Estland 2007 eine Bronzestatue zum Gedenken an die Rotarmisten entfernt hatte, was Tumulte im Land und Proteste Russlands provozierte, überfluteten plötzlich über Nacht massenhaft Zugriffsanforderungen die estnischen Server und brachten diese zum Zusammenbruch. Onlinebanking, das Lesen von Onlinezeitungen und sonstige Dienste im Netz waren nicht mehr möglich. Eine Flut programmierter Datenübermittlungen hatte das Netz lahmgelegt. In so einem Fall spricht man im Fachenglisch von „Distributed Denial of Service" (DDoS), im Fachdeutsch von „verteilter Dienstblockade". „Verteilt" deshalb, weil unzählige an sich harmlose Rechner, so genannte Zombies, von angreifenden Rechnern, dem „Botnetz", zur Überflutung der Server missbraucht werden. Auch Ihr Rechner könnte als Zombie eingesetzt werden. Sie würden es wahrscheinlich nicht merken und höchstens einen etwas verzögerten Internetzugang feststellen. Die Spuren des Angriffs in Estland führten nach Russland. Diese und andere Beispiele zeigen, dass der Cyberkrieg längst keine Zukunftsmusik mehr ist, sondern längst Realität. Angriffe verlaufen in Lichtgeschwindigkeit, können weltweit verübt werden und beschränken sich nicht nur auf den militärischen Bereich.

Cyberkrieger stehen bereit

Weltweit werden Cyberkrieger mobilisiert oder sind bereits im Einsatz. China beispielsweise hat effiziente Hackergruppen, spioniert im virtuellen Raum amerikanische Soft- und Hardware aus, kann sich selbst entsprechend verteidigen, verfügt über militärische Netzkriegseinheiten und hat bereits logische Bomben (Trojaner) in der Infrastruktur der USA gelegt. Das Land soll den USA bereits damit gedroht haben, das Stromnetz lahmzulegen, sollten sie gegen Chinas Versuche intervenieren, die Spratly-Inseln im Südchinesischen Meer unter seine Hoheit zu stellen.

> „Zunächst waren die Regierungen vieler Länder beeindruckt davon, was jemand mit dem Iran gemacht hatte, doch dann erschauderten sie und begriffen, dass so etwas auch ihnen widerfahren könnte."

Auch Russland hat bereits in der erwähnten „Bronzenacht" in Estland gezeigt, wozu es in der Lage ist. Die vermutlich aus dem KGB hervorgegangene Abteilung SSSI (Sonderfernmeldewesen und Kommunikation) betreibt Hackerschulen und verfügt ebenfalls über effiziente Netzkriegseinheiten. Deutschland besitzt seit 2006 eine solche Einheit. Im Jahr 2009 hat sie 76 Computerexperten beschäftigt. Die Hauptaufgabe der Einheit besteht darin, DDoS- und Botnetz-Attacken abzuwehren. Insgesamt sollen weltweit ca. 20–30 Staaten mit Cyberkrieg-Einheiten gerüstet sein.

Warum Cyberkrieg möglich ist

Der Cyberspace umfasst nicht nur das Internet, sondern auch andere Netzwerke sowie Geräte, Systeme, Maschinen usw., die damit verbunden sind. Angriffe sind möglich, weil das Internet fünf wesentliche Schwachstellen hat:

1. **Adresssystem**: Das so genannte Domain Name System (DNS), das jeden Adressnamen einer Nummer zuordnet, gilt als sehr unsicher. Hacker können beispielsweise Informationen manipulieren und Nutzer zu falschen Seiten führen.
2. **Border Gateway Protocol (BGP)**: Mit diesem System werden die Daten zwischen den Internet-Serviceprovidern (ISP) ausgetauscht und weitergeleitet. Ein Hacker kann problemlos die Datenströme im Netz verändern, sodass die Informationen beispielsweise woanders landen als geplant.
3. **Informationen sind kaum verschlüsselt**: Dadurch bleibt fast nichts geheim. Und selbst bei einer verschlüsselten Datenübertragung können Fremde mit einem so genannten Key Logger sämtliche Tastaturbewegungen erfassen. Selbst mit einer Radioantenne soll das möglich sein.
4. **Verbreitung von Schadprogrammen**: Das Internet ist der ideale Platz für die Verbreitung von Schadprogrammen (sogenannte Malware). Solche Programme enthalten unter anderem Viren, die das Betriebssystem eines Rechners stören und vertrauliche Informationen abgreifen können.
5. **Dezentraler Aufbau**: Wegen seines dezentralen Aufbaus lässt sich das Internet kaum kontrollieren und bietet der Kriminalität damit einen fruchtbaren Boden.

> „Wenn du im virtuellen Raum auf den Angriff der Gegenseite wartest, wirst du möglicherweise feststellen, dass der Gegner gleichzeitig mit seiner Attacke deine logischen Bomben entschärft hat."

Da Geräte, Maschinen und ganze Systeme heutzutage immer stärker über das Internet gesteuert werden, haben Hacker ein leichtes Spiel, wenn sie das öffentliche, wirtschaftliche und private Leben zum Erliegen bringen wollen. Die Stromversorgung auszuschalten, wäre relativ unproblematisch.

Schwache Verteidigung in den USA

Während die USA die stärkste Offensivkraft im Cyberkrieg besitzen, sieht es dort mit der Verteidigung vergleichsweise dürftig aus. Weder Clinton noch Bush noch Obama haben bis heute ein schlagkräftiges defensives System etablieren können. Dafür gibt es verschiedene Gründe: Zum einen ist bislang in dieser Hinsicht noch nichts wirklich Dramatisches passiert – was jedoch ein Trugschluss sein mag, denn Datenraub geschieht oft unbemerkt. Zum anderen finden die Entscheidungsträger keinen Konsens hinsichtlich der Strategie. Zudem gibt es immer ein politisches Lager, das den aktuellen Lösungsvorschlag abschmettert. Letztlich hat auch die Wirtschaft ihre Finger mit im Spiel, allen voran der Hauptwahlkampf-Financier von Georg W. Bush: Microsoft lehnt staatliche Vorschriften ab und verlangt vom Pentagon, Microsoft-Programme zu verwenden – trotz bekannter Sicherheitslücken. Speziell geschützt wird ausschließlich das Verteidigungsministerium, und zwar von der militärischen Behörde Cyber Command. Das Heimatschutzministerium kümmert sich um die anderen Einrichtungen der Bundesregierung. Der private Sektor, z. B. die Banken und Stromversorger, ist auf sich allein gestellt. Ganz anders in China: Dort werden sämtliche zur Internetinfrastruktur gehörenden Netze vom Staat kontrolliert. Der arbeitet auch in Sachen Verteidigung eng mit dem Privatsektor zusammen.

Defensive Triade

Ein effektives Verteidigungssystem für die USA muss aus drei Elementen bestehen: Schutz des Basisnetzes, Schutz des Stromnetzes und Schutz des Verteidigungsministeriums. Zum Basisnetz gehören ca. ein halbes Dutzend Internetdienstanbieter, unter ihnen AT&T, Verizon, Level 3, Qwest und Sprint. Fast der gesamte Internetverkehr läuft über diese Anbieter. Da sie eine Verbindung zu den meisten anderen Anbietern haben, reicht es, nur sie zu schützen anstatt Tausende von Einzelnetzen und -zielen. Mit einer so genannten Deep Packet Inspection lässt sich das bewerkstelligen. Sie überprüft etwa bei E-Mails Absender, Adressat und die Daten. Um den Datenschutz zu gewährleisten, sollte nicht der Staat, sondern der Internetdienstleister die Kontrollen durchführen, und zwar automatisch, damit niemand befürchten muss, seine E-Mails würden gelesen. Außerdem sollten die Anbieter ihre Kunden umgehend informieren, wenn deren Computer von Botnetzen missbraucht werden. Auch die laufende Suche nach Malware sollte zu den Pflichten der großen Anbieter gehören.

„Wir lassen nicht zu, dass Autobauer Autos ohne Sicherheitsgurte verkaufen. Die gleiche Logik sollte im Internet gelten."

Ein sicheres Stromnetz ist dann gewährleistet, wenn die Stromkonzerne keine Verbindung mehr zwischen Kontrollsystem und Internet unterhalten. Wo die Kontrollsysteme mit dem Intranet verbunden sind, sollte eine Deep Packet Inspection eingeführt werden. Ebenfalls zum Pflichtprogramm der Energieversorger gehören verschlüsselte Kontrollsignale für Generatoren, Umspannwerke und sonstige Schlüsselstellen. Beim Verteidigungsministerium empfiehlt sich eine Umstellung des Datenaustausches von Internet auf Satellit oder Laser. Diese Kanäle sind sicher gegen Hackerangriffe. Bleibt das Internet als Kanal bestehen, sollte man u. a. das Netzwerk sowie sämtliche Computer mit Firewalls, Antivirenprogrammen, Identitätsnachweisen mit Zwei-Faktoren-Authentifizierung u. Ä. schützen.

Angriff

Damit eine Offensivstrategie Erfolg hat, muss sie natürlich ebenso durchdacht sein wie eine Verteidigungsstrategie. Mit Testabwürfen von Atomwaffen kann ein Land seine Stärke demonstrieren. Bei Cyberwaffen ist das schwieriger. Natürlich könnte ein Land ein anderes übers Internet angreifen und damit auch weiteren Nationen zeigen, wozu es imstande ist. Diese Form der Abschreckung ist allerdings nicht sinnvoll, denn wird ein Angriff aufgedeckt – und das wäre ja Sinn und Zweck der Übung –, kann der Feind sofort an einer entsprechenden Abwehr arbeiten. Die beste Abschreckung beim Cyberkrieg ist immer noch ein effizientes Abwehrsystem.

„Energieunternehmen sollten gezwungen sein, unerlaubte Zugriffe auf das Kontrollnetzwerk des Stromnetzes zu verhindern."

Eine wirkungsvolle Strategie beim Cyberkrieg ist der Erstangriff. Wer zuerst zuschlägt, ist im Vorteil, denn die andere Seite verfügt u. U. noch nicht über geeignete Abwehrmechanismen. Am besten ist es darum, bereits vor dem Krieg logische Bomben in das System des Gegners zu schleusen. Genauso wichtig ist es, einen Angriff schnell zu erkennen und umgehend zu reagieren. In der Offensivstrategie muss ferner festgelegt sein, welche Kommunikationsverbindungen zerstört werden. Es könnte fatale Folgen haben, alles zu zerstören: Ist eine Einheit nämlich von ihrem Oberkommando abgeschnitten, wird sie auf eigene Faust weiterkämpfen. Es sollte immer ein Kanal für Verhandlungen bestehen bleiben, über den die Führung mit ihren Einheiten in Kontakt bleiben kann.

Cyber-Rüstungsbegrenzung

Ähnlich wie bei den Abrüstungsverträgen zum Abbau nuklearer Atomwaffen wäre auch für den Cyberkrieg ein einschränkender Vertrag empfehlenswert. Für die USA mit ihrer unzureichenden Abwehr würde sich das auf jeden Fall lohnen. Ein so genannter Cyber War Limitation Treaty (CWLT) sollte klein beginnen und später, bei gewachsenem Vertrauen, um weitere Abkommen erweitert werden. Für den Anfang wären Maßnahmen nötig wie die Einrichtung eines Zentrums zur Risikoabsenkung im Cyberspace, völkerrechtliche Normen, ein Verbot des Ersteinsatzes von Cyberwaffen gegen zivile Ziele, ein Verbot von Präventivmaßnahmen sowie ein Verbot der Manipulation von Finanzinstitutsdaten. Auch sollten sich die Unterzeichnerstaaten verpflichten, gegen Hackerangriffe vorzugehen, die innerhalb der eigenen Grenzen gestartet werden. Ein im besagten Zentrum stationiertes Computerforensikteam kann überprüfen, ob sich die Unterzeichner an den Vertrag halten. Bei Verstößen müssen strenge Sanktionen verhängt werden, z. B. Einreiseverbote für ausgewählte Personen oder die Einstellung des Internetverkehrs in dem betreffenden Land.

Über die Autoren

Richard A. Clarke beriet über drei Jahrzehnte im Weißen Haus, im State Department und im Pentagon vier US-Präsidenten. Unter Bill Clinton fungierte er als Bundeskoordinator für die nationale Sicherheit. Heute lehrt er an der Kennedy School of Government der Harvard University. Dort studierte auch Mitautor **Robert K. Knake**. Der Experte für Internetkriminalität ist heute Mitarbeiter des Council on Foreign Relations.