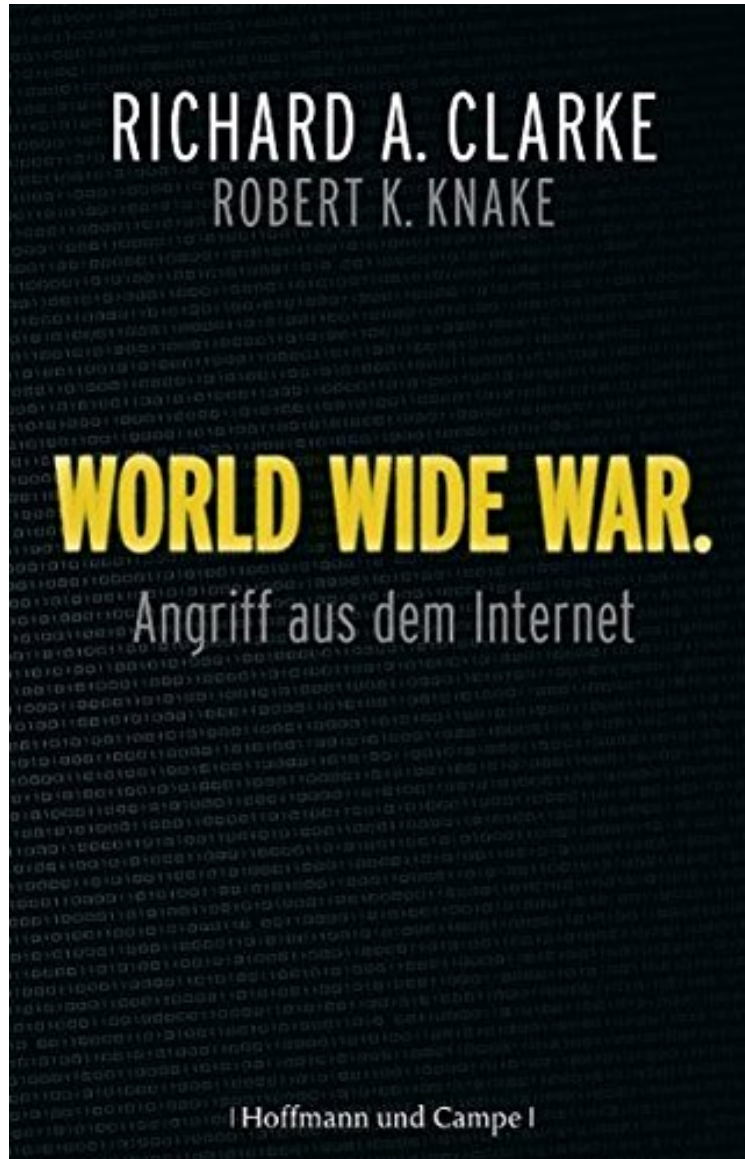


[Read free ebook] World Wide War: Angriff aus dem Internet (Zeitgeschichte)

World Wide War: Angriff aus dem Internet (Zeitgeschichte)

Von Richard A. Clarke, Robert A. Knake
audiobook / *ebooks / Download PDF / ePub / DOC



DOWNLOAD



+

READ ONLINE

Produktinformation - Verkaufsrang: #572718 in BcherVerffentlicht am: 2011-03-04Abmessungen: 8.50 x 1.34b x 5.83l, Einband: Gebundene Ausgabe352 Seiten | File size: 43.Mb

Von Richard A. Clarke, Robert A. Knake : World Wide War: Angriff aus dem Internet (Zeitgeschichte) before purchasing it in order to gage whether or not it would be worth my time, and all praised World Wide War: Angriff aus dem Internet (Zeitgeschichte):

KundenrezensionenHilfreichste Kundenrezensionen1 von 1 Kunden fanden die folgende Rezension hilfreich. Die USA im World Wide WarVon Gerald TrimmelDie bereits verffentlichten Rezensionen gehen ausfhrlich auf die positiven Aspekte des Buches ein: die Errterung eines Paradigmenwechsels vom klassischen Kriegsszenario zum

sogenannten "Cyberwar". Der hochrangige US-Militärstrategie Richard A. Clarke und sein jüngerer Ko-Autor Robert K. Knake beschreiben sehr anschaulich und detailliert, wie auf dem "virtuellen Schlachtfeld" zukünftig Krieg ausgetragen werden könnten und welche nationalen und globalen Folgen sich dadurch ergeben würden - etwa der Zusammenbruch der Energieversorgung, des Transportwesens, des Finanzwesens und der Kommunikation. Unzählige vor allem zivile Todesopfer wären die Folge. Während die ersten Kapitel noch den Anschein eines gut recherchierten Sachbuchs erwecken, das allgemein verständlich technologische und politische Aspekte der virtuellen Kriegsführung erklärt, steht schließlich nur noch eine konkrete Frage dominant im Vordergrund: "Was müssen WIR, die USA, tun, um die Bedrohungen virtueller Angriffe effizient abwehren zu können?" Angesichts der Enthüllungen von Edward Snowden sind wir - die deutschsprachigen Leser dieser Ausgabe - für eine derartige Bruchlinie in dem bereits 2011 in deutscher Übersetzung erschienenen Buch sicherlich sensibler geworden. Der Titel des Buches sollte daher heißen: "Die USA im World Wide War: Bedrohungspotenziale und Krisenstrategien". Zusammenfassend stelle ich fest: die Einführung in die Thematik ist durchaus gelungen. Nach der Veröffentlichung geheimer Dossiers durch Edward Snowden über den globalen "virtuellen Präventivkrieg" der USA ist das Buch auch als Quelle für militärstrategische Überlegungen der USA nur mehr bedingt interessant. Ob das daher heute noch den Kauf rechtfertigt, darf eher bezweifelt werden.

6 von 6 Kunden fanden die folgende Rezension hilfreich. Lächer im Netz Von Konrad Schlegel Eine auch für den Nichtinformatiker gut verständliche Darstellung der Risiken, die durch den in alle Bereiche durchdringenden Einsatz des Internets entstehen. Die Autoren beschreiben die Verwundbarkeit ziviler Systeme, wie zum Beispiel der Energieversorgung, durch überraschende gegnerische Angriffe und analysieren Sicherheitslücken auch im militärischen und nachrichtendienstlichen Bereich. Richard A. Clarke war Sicherheitsberater mehrerer amerikanischer Präsidenten. Er kennt die Sicherheitsstrukturen und deren Lücken seines Landes ebenso genau wie die verschiedenen Standpunkte zu militärischen Aspekten der Internetnutzung. Er erläutert an Beispielen, wie groß die Bedeutung von Computerattacken bei den letzten militärischen Auseinandersetzungen bereits war, obwohl in der Öffentlichkeit davon wenig bekannt wurde. Die Herausforderungen durch militärisch nutzbare Informationstechnologie werden mit denen durch die Atomwaffen während des Kalten Krieges verglichen. Dies gilt nicht nur für die taktischen und strategischen Überlegungen, sondern auch für die Politik und die Notwendigkeit der Weiterentwicklung des Völkerrechts. Die Autoren Clarke und Knake vertreten die Ansicht, dass eine weitgehend offene Struktur des Internets ein erhebliches Sicherheitsrisiko darstellt, welches die Vereinigten Staaten im Falle eines Cyber-Angriffes leichter verwundbar machen würden als potenzielle Gegner. Davon ausgehend fordern sie größere Verteidigungsanstrengungen in diesem Bereich. Auch wenn man sich sicher sein kann, dass die Autoren die bedrohlichsten Schwächen der amerikanischen Netzstruktur schon aus Sicherheitsgründen verheimlicht haben dürften, so lernt der Leser durch dieses Buch die Denkweise und Entscheidungsstrukturen amerikanischer Regierungen viel genauer kennen.

Konrad Schlegel 5 von 5 Kunden fanden die folgende Rezension hilfreich. Cyberwar ist viel gefährlicher als nur das Verunstalten von Websites Von Aiden Pearce Der Begriff Cyberwar ist spätestens seit Stuxnet in der breiten Öffentlichkeit angekommen. Täglich hören wir in den Nachrichten von Hacktivisten wie Anonymous die wieder irgendwas geleakt oder DDoS-Attacken gestartet haben. Die wenigsten wissen aber was hinter dem Begriff Cyberwar steht bzw. wie er bereits stattfindet und was uns noch erwarten könnte. Richard Clarke beginnt in diesem Buch mit einem israelischen Luftangriff auf Syrien der vermutlich in Kombination eines Cyberschlages durchgeführt wurde, da die Kampfflugzeuge (keine Tarnkappenbomber) ja normalerweise vom Radar hätten erfasst werden müssen. Es wird auf die Schwachstellen im Netz und der eingesetzten Software eingegangen, die allerdings nicht sehr weit ins Detail gehen und von Nichtinformatikern leicht zu verstehen ist. Aber selbst wenn heute Windows nicht mehr so unsicher ist wie noch vor ein paar Jahren gibt es noch genügend Schwachpunkte und es wird auch erwähnt, dass Microsoft von China dazu gezwungen wurde den Windows-Code auszuhändigen, der von chinesischen Spezialisten sicher genau nach Schwachstellen durchforstet wurde. Die wirkliche Gefahr im Cyberwar ist aber der Angriff auf die Infrastruktur eines Landes wie die Stromnetze. Oft wurden schon lange vor dem Angriff "logische Bomben" an kritischen Stellen platziert, die per Kommando in Lichtgeschwindigkeit aktiviert werden können. Stark technisierte Staaten wie die USA sind natürlich besonders betroffen. Nordkorea hingegen verfügt über starke Angriffskapazitäten ist aber selbst fast immun, da es dort kaum Vernetzung gibt. Ein großer Teil des Buches bezieht sich speziell auf Verteidigungsstrategien der USA und mögliche Konventionen zur Verwendung/Vermeidung von Cyberwaffen und Analogien zum Atomwaffeneinsatz. Fazit: Ein generell sehr informativ aufgebautes Buch mit viel USA-Bezug. Während des Lesens wurde mir auch wiedermal bewusst, dass mir jemand in Sekundenschnelle vermutlich meine Bücher vom Kindle löschen könnte und es ist beängstigend wenn man bedenkt wie verwundbar unsere gesamte Gesellschaft gegen Cyberangriffe ist.

Pressestimmen Das exzellent geschriebene und hochspannende Buch wirft die Frage auf, ob eine totale Vernetzung aller Lebensbereiche wirklich sinnvoll ist. (balance, 07.2011) Das vorliegende Buch aus Amerika gibt, mit vielen konkreten Beispielen belegt, einen guten und an manchen Stellen wirklich erschreckenden Überblick über diesen 'World Wide War' mit seinen Angriffen aus dem Internet ... (Buchtips.net) Das Buch informiert den Leser nicht nur detailliert

ber die US-Cyberkrieger. Vielmehr erlaubt es auch einen Blick auf die sicherheitspolitischen Diskussionen ber knftige virtuelle Schlachtfelder, mgliche Verteidigungsmechanismen und einen 'Cyberfrieden'. (Aschot Manutscharjan Bundeswehr aktuell, 02.05.2011)Die Motive, Ziele und Waffen der Cyberstrategen werden auch fr Leser, die kaum mit der Materie Cyberspace vertraut sind, verstndlich geschildert. (Das Archiv, Magazin fr Kommunikationsgeschichte, 04.2011)World Wide War' ist das erste Buch, das ber den aktuellen Stand dieser globalen Entwicklung informiert (Das Buch-Magazin)Die Lektre eignet sich fr jedermann, der wissen will, was ohne sein Wissen mit seinem Computer passiert oder passieren knnte. (Tom Goeller Deutschlandradio) przise und klug (Vera Lin Deutschlandradio) eloquent begrndet (Stefan Grund DIE WELT)... packend geschrieben (NDR Info)... ein Sachbuch-Thriller der Meisterklasse (readme.de) so faktenreich beschrieben, dass sich das nchterne Sachbuch wie ein spannender Thriller liest. (Gordon Bolduan Technology , 05.2011)KurzbeschreibungStell dir vor, es ist Krieg und keiner geht hin - nicht weil keiner will, sondern weil nichts mehr funktioniert. Amerikas Sicherheitsexperte Nr. 1 warnt: Das Internet ist nicht nur ein Segen, sondern auch eine Quelle neuer Gefahren, gegen die effektivere Schutzmanahmen ergriffen werden mssen. Der weltweite Netzkrieg hat begonnen. Ein auftrttelndes Buch ber Cyberstrategen, ihre Motive, Ziele und Waffen. Seitdem das World Wide Web existiert, gibt es auch die Mglichkeit, in fremden Rechnern Schaden anzurichten. Doch seit Ende 2008 nehmen die Attacken explosionsartig zu, und sie gelten immer hufiger der Sabotage vernetzter Groanlagen. Sptestens seit der Entdeckung des Computerwurms Stuxnet im Sommer 2010 berichten die Medien Tag fr Tag ber feindliche Aktivitten im Internet - und ber die Tatsache, dass die Industrienationen schlecht auf sie vorbereitet sind. World Wide War ist das erste Buch, das ber den aktuellen Stand dieser globalen Entwicklung informiert. 'Knnten wir diesen Geist wieder in die Flasche sperren, sollten wir das tun', schreiben die Autoren. 'Aber wir knnen es nicht.'ber den Autor und weitere MitwirkendeRichard A. Clarke, geboren 1951, war mehr als drei Jahrzehnte lang im Weien Haus, im State Department und im Pentagon als Berater fr vier US-Prsidenten ttig. Bill Clinton ernannte ihn zum Bundeskoordinator fr die nationale Sicherheit. Nach den Terroranschlgan am 11. September 2001 leitete er den Krisenstab des Weien Hauses. Im Mrz 2003 legte er sein Amt nieder und verffentlichte 2004 den Bestseller 'Against All Enemies'. Clarke ist heute Dozent an der Kennedy School of Government der Harvard University und leitet die Firma Good Harbour Consulting. Robert K. Knake studierte an der Kennedy School of Government der Harvard University Politikwissenschaften, Schwerpunkt Internationale Sicherheit, und ist Mitarbeiter des Council on Foreign Relations, wo er sich auf Internetkriminalitt spezialisiert hat.