Medienimpulse
ISSN 2307-3187
Jg. 53, Nr. 1, 2015

Rezension: World Wide War: Angriff aus dem Internet/Cyber War: The Next Threat to National Security and What to Do About It von Richard A. Clarke und Robert K. Knake/by Richard A. Clarke and Robert K. Knake

Karl H. Stingeder

Je breiter der Infrastruktur-Anschluss eines Landes an das World Wide Web, desto größer die Angriffsfläche im Fall eines Netzkriegs. Die Messung der virtuellen Kampfkraft erfolgt auf Basis von drei Faktoren: Offensivkraft, Defensivfähigkeit und die Abhängigkeit vom Internet. Die USA verfügen als "Supermacht" zwar über die größte virtuelle Offensivkraft, gleichzeitig steht die Nation Cyberangriffen sehr verwundbar gegenüber. Dagegen sind in Nordkorea kaum Systeme vom Internet abhängig. Obwohl die offensiven Netzkriegskapazitäten Nordkoreas verhältnismäßig gering

sind, präsentiert sich die virtuelle Kampfkraft des nordkoreanischen Regimes in Bestform. Die Verwundbarkeit ziviler Systeme, insbesondere der Energieversorgung, muss in direkter Korrelation mit deren Anknüpfung an das Internet betrachtet werden.

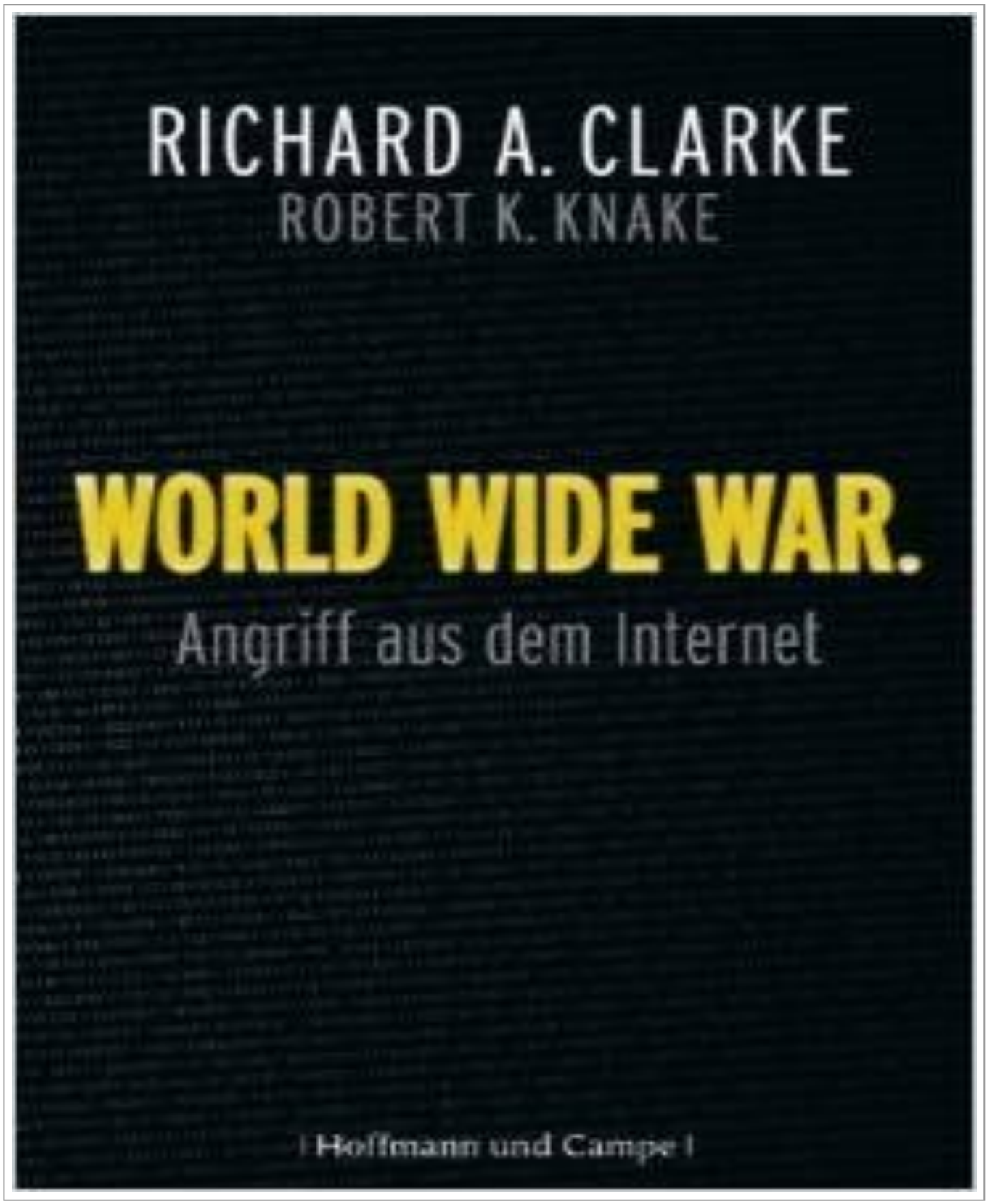
The more broadly connected a country's infrastructure and energy distribution, the greater its vulnerability in the event of a cyber war. Measuring this virtual fighting power is based on three factors: offensive and defensive strength, as well as dependency on the Internet. As a superpower, the USA has the greatest virtual offensive strength available. At the same time, the nation is most susceptible to cyber attacks and therefore most vulnerable. By contrast, North Korea's offensive cyber fighting power is relatively small, but its overall cyber war capabilities are cutting-edge. The vulnerability of civil systems, especially power supply, must be viewed in direct correlation to their connection to the Internet.

Verlag: Hoffmann und Campe Verlag
Erscheinungsdatum: 2011
Erscheinungsort: Hamburg
ISBN: 978-3455501865
Deutsch, 274 Seiten

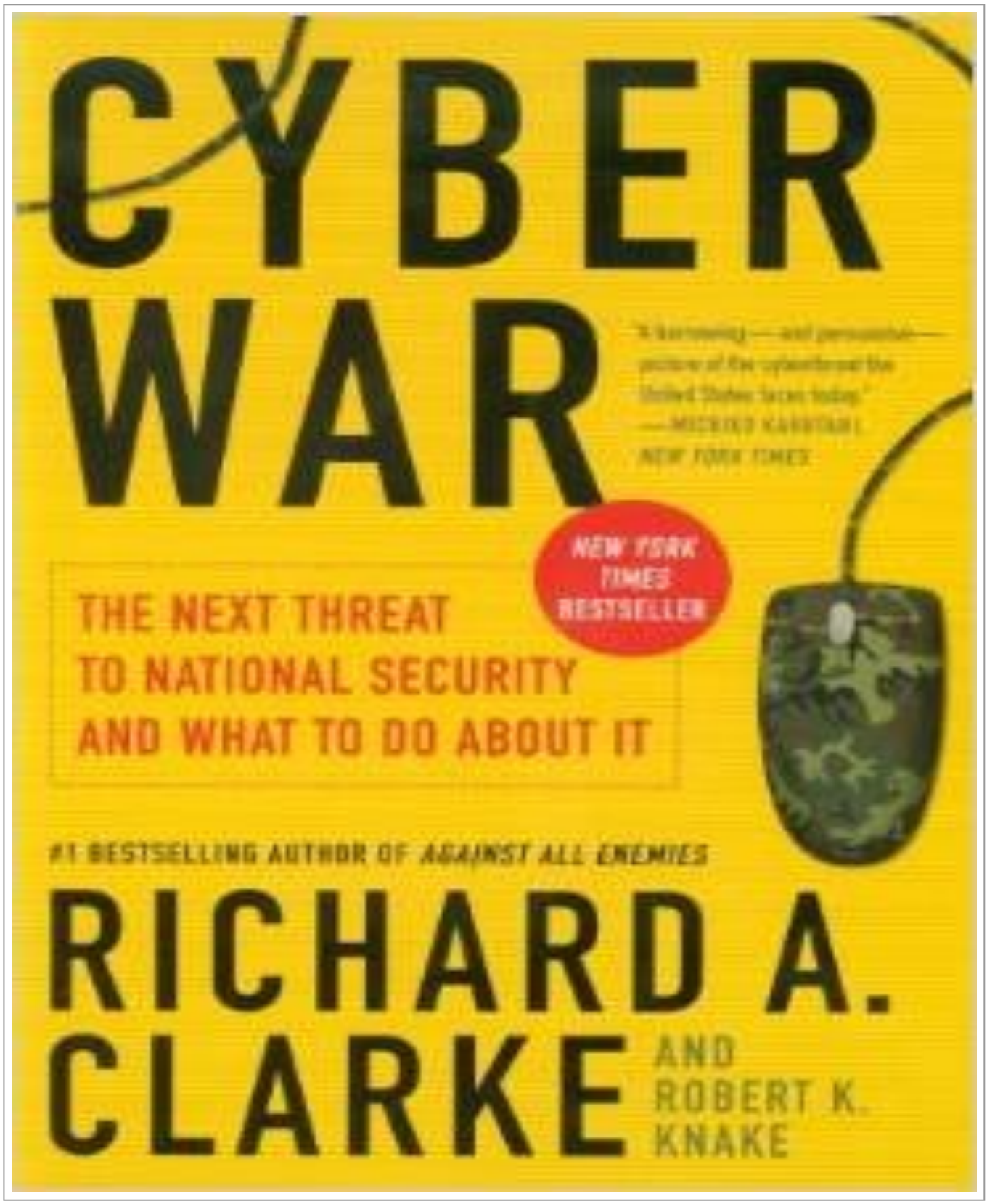
Publisher: Hoffmann und Campe Verlag
Year of publication: 2011
Place of publication: Hamburg
ISBN: 978-3455501865
German, 274 Pages

English original version:
Publisher: ecco; Reprint edition
Year of publication: 2012 (2010)
Place of Publication: New York

ISBN: 978-0061962240
English, 320 Pages


RICHARD A. CLARKE
ROBERT K. KNAKE
WORLD WIDE WAR.
Angriff aus dem Internet
Hoffmann und Campe

Cover: World Wide War,
von Richard A. Clarke und Robert K. Knake,
Quelle: Amazon


CYBER WAR
"A harrowing — and persuasive — picture of the cyberthreat the United States faces today."
— MICHIKO KAKUTANI, NEW YORK TIMES
NEW YORK TIMES BESTSELLER
THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT
#1 BESTSELLING AUTHOR OF AGAINST ALL ENEMIES
RICHARD A. CLARKE
AND ROBERT K. KNAKE

Cover: Cyber War,
von Richard A. Clarke und Robert K. Knake,
Quelle: Amazon

Im Film "WarGames" (1983)[1] gelingt es David, einem jugendlichen Hacker-Ausnahmetalent, die virtuelle Hintertüre in den militärischen Zentralrechner "Joshua" aufzuspüren und zu durchbrechen. Daraufhin fordert der Supercomputer David zu einem Duell heraus. In der Sichtweise Davids handelt es sich um ein spielerisches Szenario rund um einen nuklearen Weltkrieg zwischen Amerika und Russland. David nimmt die Herausforderung an, doch das "Spiel" entpuppt sich als tödlicher Ernst: die letzte Konsequenz wäre der reale atomare Holocaust. Während der Countdown läuft, setzt David alle Hebel in Bewegung um einen möglichen Nuklearkrieg zu verhindern. Was vor rund dreißig Jahren, lange vor der breitenwirksamen Etablierung des Internet und des World Wide Webs sicherlich wie weit entfernte Zukunftsmusik klang, ist nun Realität. Inwieweit kann das Internets im Rahmen unseres "vernetzten" Alltags Schaden verursachen?

Spätestens seit der weltweiten Verbreitung des Wurms namens Stuxnet[2] sowie seit den Enthüllungen Edward Snowdens (vgl. Internetquelle[3]) wurde die Öffentlichkeit wachgerüttelt. Zudem veranschaulichen regelmäßige Berichte über Angriffe auf Regierungen oder Konzerne die große Reichweite des Internets. Im Dezember 2014 bezichtigten die USA öffentlich Nordkorea einer Cyberattacke (vgl. Internetquelle[4]). Zuvor sah der Medienkonzern Sony Entertainment Pictures sich in Folge eines Hacker-Angriffs gezwungen den für Weihnachten 2014 veranschlagten Kinostart von "The Interview" (2014, vgl. Internetquelle[5]) zu verschieben. Die Filmhandlung dreht sich um zwei Journalisten, die sich einen Interviewtermin mit dem nordkoreanischen Diktator Kim Jong-un verschaffen und im Zuge dessen vom CIA für einen Anschlag auf den Führer Nordkoreas rekrutiert werden.

"The Interview" sollte als Kinokomödie zur Weihnachtszeit die Kassen klingeln lassen, eine Hacker-Attacke wusste dies erfolgreich zu verhindern. Obwohl in diesem Fall kein großer Schaden angerichtet wurde, verdeutlicht dieses Beispiel die politische Reichweite von Cyber-Angriffen. Die Autoren stellen im Buch folgende Fragen: Was steht hinter dem Begriff Cyberwar, wie funktioniert dieser "World Wide War" und welche Bedeutung hat dies für uns angesichts der Tendenz der Vernetzung und Steuerung wichtiger "Offline"-Versorgungssysteme über das Internet? Richard Clarke, einer der beiden Autoren, war drei Jahrzehnte Sicherheitsberater des Weißen Hauses. Somit ist nachvollziehbar, dass
das Buch die Thematik aus dem Blickwinkel der USA betrachtet. Die Studie kann dank zahlreicher Fallbeispiele sowie in Folge einprägsamer Begriffserklärungen (z.B. "Würmer", "logische Bomben", "Pufferüberlauf", etc.) – sowohl im Fließtext als auch als mittels eines Glossars zum Schluss des Buchs – als einsteigerfreundlich bewertet werden.

Im Auftakt-Kapitel "Probeläufe" veranschaulichen die Autoren die Rolle des Cyberwars für die militärische Kriegsführung am Beispiel Nordkoreas Cyberattacke im Jahr 2009. Das Regime testete am 4. Juli 2009, dem amerikanischen Unabhängigkeitstag, eine Kurzstreckenrakete. Eingeleitet wurde diese Drohgebärde jedoch von einer verschlüsselten Botschaft eines nordkoreanischen Agenten, welche etwa 40.000 Computer in aller Welt mit einem Virus infizierte. Dieser sogenannte "Botnetvirus" (Internetquelle[6]) infizierte Rechner und veranlasste diese dazu amerikanische und südkoreanische Website "anzupingen". Sobald die infizierten Rechner eingeschaltet wurden, konnte man beobachten wie bestimmte Websites mit zahlreichen Anfragen überhäuft wurden. Ziel war es die Server zur dazugehörigen Website durch zu hohen Datenzustrom förmlich in die Knie zu zwingen. Diese Form der Netzattacke ist auch als DDoS bekannt (vgl. Internetquelle[7]). Die Schäden hielten sich in Grenzen. Daher sprechen die Autoren in diesem Zusammenhang von

einem "Schuss vor dem Bug" durch Nordkorea. Dennoch wurde mit dieser Cyberattacke deutlich wie einfach und effektiv gleichermaßen die Reichweite des Internets genutzt werden kann um gezielt Schäden anzurichten. (vgl. Clarke/Knake 2011: 42–44)

An Hand dieses Beispiels kann nun der Kreis zur eingangs gezogenen Parallele zum Film "WarGames" geschlossen werden: die aus der Filmdystopie bekannten Gefahrenpotentiale sind dreißig Jahre später zur Realität geworden und greifbar. Und auch wenn – im Gegensatz zu "WarGames" – kein nuklearer Vernichtungsschlag unmittelbar bevorstehen sollte, so wird die zunehmende Netzabhängigkeit von Basissystemen, welche die Energieverteilung oder den Verkehrsfluss steuern, immer augenscheinlicher. Bemerkenswert ist in diesem Kontext der "Präventiveinsatz" bestimmter Netzwaffen. Häufig werden lange vor tatsächlichen Konflikten, welche Cyberattacken zur Folge haben sogenannte "logische Bomben" in elektronischen Systemen deponiert. Diese "heimlichen Sprengkörper" können auf Kommando aktiviert werden und betroffene Systeme per Knopfdruck lahmlegen oder zerstören. So geschehen im Zuge der Stuxnet-Attacke 2010, welcher gegen die Uran-Zentrifugen des Irans gerichtet waren. (vgl. Internetquelle[8])

Somit gilt die Maxime: je höher der Grad der Technisierung, je verbreiteter die Vernetzung mit dem Internet, desto größer die Angriffsfläche im Fall eines Cyberwars. Die Autoren sprechen in diesem Kontext von der Messung der "virtuellen Kampfkraft". Festgemacht wird diese an Hand von drei Faktoren: Offensivkraft, Defensivfähigkeit und die Abhängigkeit vom Internet. Um die Wechselwirkung zwischen diesen drei Aspekten zu verdeutlichen, haben die Autoren eine Tabelle erstellt und jedem Land einen Punkt zwischen eins und neun pro Faktor (Offensivkraft, Defensivfähigkeit und die Abhängigkeit vom Internet) zugeordnet. Die Resultate dieses Bewertungsschemas führen eindrucksvoll vor Augen, dass die USA als "Supermacht" zwar über die größte virtuelle Offensivkraft verfügen (daher wurde mit acht Punkten fast der Höchstwert zugeteilt), gleichzeitig jedoch Cyberangriffen am

verwundbarsten gegenüberstehen: Die virtuelle Verteidigungsfähigkeit der USA wurde mit dem Wert eins bemessen. China findet sich im Mittelfeld dieser Bewertung der Buchautoren wieder. Das Land hat gemäß den Autoren Vorkehrungen getroffen um im Ernstfall seine Netze vom Cyberspace abzukapseln. (vgl. Clarke/Knake 2011: 194–195)

Land	Virtuelle Offensivkraft	Abhängigkeit von vernetzen Systemen	Virtuelle Verteidigungsfähigkeit	Gesamt
USA	8	2	1	11
Russland	7	5	4	16
China	5	4	6	15
Iran	4	5	3	12
Nordkorea	2	9	7	18

Abb 1: Clarke/Knake 2011: 195, virtuelle Kampfkraft

Im Gegensatz zu den sich stetig verschlechternden konventionellen Militärkapazitäten Nordkoreas (vgl. Stingeder 2009: 61–89 sowie vgl. Stingeder 2010: 69–100)[9]], präsentiert sich die virtuelle Kampfkraft des nordkoreanischen Regimes in Ihrer Gesamtheit betrachtet in Bestform – mit insgesamt 18 Bewertungspunkten. Wohlgemerkt nicht im Bereich der Netzkrieg-Offensivfähigkeiten, hier bilde Nordkorea – auf Basis der Bemessung der Buchautoren Clarke und Knake – mit zwei Punkten das Schlusslicht. Die USA nehmen bei den Offensivfähigkeiten demnach – mit acht Punkten – die Spitzenposition ein, gefolgt von Russland, China und

dem Iran. Summa summarum biete Nordkorea schlichtweg eine zu geringe Netzkriegs-Angriffsfläche sowie eine zu geringe Abhängigkeit vom Internet. (vgl. Clarke/Knake 2011: 194–196)

"Nordkorea kann seine sehr beschränkten Verbindungen zum Internet noch leichter und effektiver kappen als China. Obendrein sind in Nordkorea derart wenige Systeme vom Internet abhängig, dass ein massiver elektronischer Angriff auf dieses Land praktisch keine Schäden verursachen würde." (ebd.: 196). Dreht man den Spieß um, kehrt sich die Lage ins Gegenteil: was wäre wenn es einem Angreifer gelänge mittels einer virtuelle Attacke das Stromnetz der USA an einer verwundbarer Stelle zu treffen? Die Autoren beantworten diese Frage mit einer fatalistisch geprägten Schilderung der Folgewirkungen. Generell ist die Motivation der mancherorts etwas überbordenden Ausschmückung wahrscheinlicher Unheilszenarien die in der Sichtweise der Autoren nachhaltig forcierte und daher fahrlässige Verwundbarkeit ziviler Systeme der Vereinigten Staaten. Dies gilt insbesondere für Anknüpfung der Energieversorgung an das Internet.

"World Wide War: Angriff aus dem Internet" bietet einen zugänglichen Einstieg in die Welt der strategischen Cybersecurity und der Cyberkriegsführung. Auch dürfen sich die Autoren hoch anrechnen lassen, dass sie auf Basis ihrer Erfahrung im Dienst der US-Regierung, einen Spagat versuchen: einerseits möchten sie politische Hintergründe von dargelegten Konfliktkonstellationen im Kontext mit den technischen Kampfmitteln des Netzkriegs veranschaulichen, andererseits – sozusagen auf technischer Metaebene – beleuchten sie grundlegende Schwachstellen des Internets. Auch legen sie Wert darauf die Schwächen eingesetzter Software (z.B. Windows) hervorzuheben. Das erklärte Ziel ist es den LeserInnen Einblicke in aktuelle sicherheitstechnische Herausforderungen des Cyberspace zu bieten. Bis auf wenige Abstriche kann dieses Wagnis als gelungen bezeichnet werden. Bedingt durch den US-dominierten Blickwinkel und die Teils viel zu emotionsgeladene Rhetorik, wirken manche Kapitel wie flammende Überzeugungsreden, adressiert an den US-Präsidenten.

Fazit: "World Wide War: Angriff aus dem Internet" schafft es auch für NichtinformatikerInnen und Nicht-Websecurity-ExpertInnen die Risiken, welche durch den alle Bereiche durchdringenden Einsatz des Internets entstehen, gut greifbar zu machen. Nicht absehen konnten die Autoren die späteren Enthüllungen Edward Snowdens. Nach Snowdens Veröffentlichung geheimer NSA-Dossiers über den globalen "virtuellen Präventivkrieg" der USA im Jahr 2013 (vgl. Internetquelle[10]), hat das 2011 erschiene Buch als eines der Basiswerke für Cyberkriegsführung an Bedeutung größtenteils eingebüßt. Nichts geändert haben Snowdens Enthüllungen jedoch am Buch in seiner Rolle als gutes Cyberwar-Einstiegswerk sowie maßgebliches Mahnmal für den vorsichtigeren Umgang der Vernetzung sensibler Schlüsselsysteme.

In the movie "WarGames" (1983)[11], David, a young hacker prodigy, succeeds in accessing a loophole to the military supercomputer "Joshua". The computer challenges David to a duel. In the young hacker’s eyes, this is at first a game scenario involving a nuclear world war between America and Russia. He accepts the challenge, but the game turns out to be deadly serious: a real nuclear holocaust would be the ultimate consequence. For this reason, David pulls out all the stops to avoid possible nuclear war. What must have seemed a long way off thirty years ago, long before the establishment of the Internet and the World Wide Web, is now reality. To what extent can the Internet, as part of our "connected" everyday life, be used to cause harm?

The general public has been shaken awaken at the latest since the worldwide circulation of the Stuxnet[12] worm, as well as the uncovering of secret NSA dossiers by Edward Snowden (cf. Internet source[13]). Furthermore, regular reports about cyber attacks directed at governments or corporations have illustrated just how far the Internet reaches. In December 2014, the USA publicly accused North Korea of hacking attacks[14] against Sony Entertainment Pictures. Sony had previously postponed the theatrical release of "The Interview" (2014, cf. Internet source[15]) as a direct result of the cyber attacks. The plot of "The Interview" involves two journalists who manage to secure an

interview with North Korea's dictator Kim Jong-un. As a result, the CIA recruits them with the goal of assassinating Kim Jong-un.

"The Interview" is a comedy and should have made the cash tills ring at Christmas, but a hacker attack successfully prevented this. Although there was no extensive damage, it illustrates the political range of cyber attacks. In the book, the authors pose the following questions: What is behind the term 'cyber war'; how does this 'world wide war' function; and what repercussions might this have in light of the trend towards interconnectedness and control of important "offline" supply systems via the Internet? Richard Clarke, one of the authors, was a security advisor to the White House for three decades, so it is understandable that the topic should be viewed through the lens of the US. However, the study can be rated as beginner-friendly, thanks to numerous example cases and memorable definitions (e.g. of "worms", "logical bombs", "puffer overflow", etc.). This applies to the body text as well as to the glossary at the end of the book.

In the chapter "Test Run", the authors illustrate the role of cyber war in military warfare by using the example of North Korea's cyber attack in 2009. Prior to the incident, the regime tested a short-range missile on 4th of July, Independence Day. This aggressive gesture was instigated through an encrypted message from a North Korean agent, which infected 40,000 computers worldwide with a virus. This so-called "Botnet Virus" (cf. Internet source[16]) caused all affected computers to ping American and South Korean websites. As soon as the infected computers were switched on, all contacted websites and computers were cluttered with requests. The goal was to force the servers of targeted websites down due to the high data stream. This attack is also referred to as a distributed denial of service, or DDoS. (cf. Internet source[17]). However, in this case the damage was limited. In this context, the authors therefore talk about a 'shot across the bow' by North Korea. In any case, this cyber attack made clear how easy and how effectively the scope of the Internet can be exploited to wreak deliberate damage. (cf. Clarke/Knake 2011: 42–44)

With this example, we come back full circle to the parallel drawn earlier on between "WarGames" and increasing interconnectedness. Essentially, the potential risks presented in the dystopian movie have become a tangible reality thirty years later. Even if – unlike "WarGames" – we are not facing nuclear devastation, the dangers of growing Internet dependence for energy supply or traffic control are becoming increasingly apparent. What is most remarkable in this context is the preventive usage of certain cyber weapons. It is not unusual for so-called "logical bombs" to be deployed, as in the 2010 Stuxnet cyber attack directed against Iran's uranium centrifuges. (cf. Internet source[18]) These "stealthy explosives" are usually infiltrated in electronic systems way ahead of actual conflicts and are activated remotely at the touch of a button. Systems affected are either incapacitated or destroyed.

The following maxim thus applies: the more connected a country's infrastructure and energy distribution, the greater its vulnerability in the event of a cyber war. In this context, the authors talk about measuring "virtual fighting power". This is exemplifed by three factors: cyber offensive and cyber defensive strength as well as dependency on connected systems. In order to illustrate the reciprocity between these three aspects, the authors created a table and have assigned each country a value between one and nine per factor. The strengths and weaknesses of the USA, China, Russia and North Korea are therefore quantified accordingly. The results clearly demonstrate that the USA as "superpower" has the greatest virtual offensive strength at hand (hence the almost peak score of eight). At the same time, the nation is most susceptible to cyber attacks and therefore most vulnerable: its virtual defensibility has been rated as just one out of nine. China is mid-table according to this scoring: according to the authors, it has made arrangements to cut its networks off from cyberspace in case of a conflict. (cf. Clarke/Knake 2011: 194–195)

Country	Cyber Offensive	Cyber Defensive	Dependency on Connected Systems	Sum Total
USA	8	2	1	11
Russia	7	5	4	16
China	5	4	6	15
Iran	4	5	3	12
North Korea	2	9	7	18

Ill. 1: Clarke/Knake 2011: 195, Virtual Fighting Power

Contrary to North Korea's steadily deteriorating conventional military capacity (cf. Stingeder 2009: 61–89 and Stingeder cf. 2010: 69–100)[19], its overall cyber combat power is at its best and has been assigned 18 points by the authors. Please note that this does not apply to North Korea's offensive cyber fighting power, which is relatively small – the authors rated this only a two. In fact, in regards to offensive capability, the regime comes last, according to the authors Clarke and Knake. Instead the USA takes pride of place, with eight points, followed by Russia, China and Iran. Despite its weakness in regards to offensive cyber warfare, North Korea would simply offer an insufficient vulnerability for cyber war as well as an insufficient dependence on the Internet. (cf. Clarke/Knake 2011: 194–196) All told, North Korea offers a low target area in the event of cyber war, and little dependency on the Internet.

According to Clarke and Knake, North Korea is capable of cutting off its ties to the Internet more easily and more effectively than China. What is more, in North Korea few systems of this type are dependent on the Internet, so a massive electronic attack would not do any significant harm. (cf. ibid) If the tables are turned, the situation reverses: what if a cyber assault could be accomplished and resulted in critically damaging the US power grid? The authors answer this question with a fatalistic portrayal of possible consequences. In general, the in some places rather exuberant embellishment of probable scenarios can be interpreted as a direct result of the authors' view on the reckless vulnerability of civil systems in the USA. This applies in particular to the connection of the power supply to the Internet.

"Cyber War: The Next Threat to National Security and What to Do About It" offers an accessible entry point to the world of strategic cyber security and cyber warfare. What is more, the authors can be credited for their attempt at balance (on the grounds of Clarke's longstanding experience in the White House): on the one hand, they aim to illustrate the political background of the conflicts discussed in context with the technical weapons of cyber warfare; on the other hand – you could say on a meta level – they shed light on the basic weak points of the Internet. The authors also place value on highlighting the weaknesses of widely deployed software (e.g. Windows). The declared goal is to grant readers insights into current cyber security challenges. Apart from a few exceptions, this endeavor can be evaluated as mission accomplished. Due to the US-dominated viewpoint and the at times emotionally-charged rhetoric, some chapters may come across as blazing monologues aimed at persuading the US president.

Bottom Line: "Cyber War: The Next Threat to National Security and What to Do About It" accentuates and explains the risks involved in the all-pervasive Internet. However, it does so in a way that is also accessible to laypersons. The authors could not, of course, foresee Edward Snowden's release of secret NSA dossiers in 2013, which illuminated the global and "virtual preventive war" of the US (cf. Internet source[20]). Since then, the

book has largely lost its value as one of the standard reference works for cyber warfare. That said, this circumstance has not affected the book's role as a fine entry point for learning about cyber warfare, nor as an essential reminder of the need for a more cautious handling of cross-linking sensitive key systems.

---

[1]IMDb (2015): WarGames 1983, online unter: http://www.imdb.com/title/tt0086567/?ref_=fn_al_tt_1 (letzer Zugriff: 05.02.2015).

[2]Kushner, David (2013): The Real Story of Stuxnet, online unter: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (letzer Zugriff: 07.02.2015).

[3]Vanityfair.com (2013): The Snowden Saga: A Shadowland of Secrets and Light, online unter: http://usnews.nbcnews.com/_news/2013/06/10/18882615-what-we-know-about-nsa-leaker-edward-snowden?lite (letzer Zugriff: 15.01.2015).

[4]Time.com (2014): U.S. Sees North Korea as Culprit in Sony Hack, online unter: http://time.com/3639237/sony-hack-north-korea-the-interview (letzer Zugriff: 15.02.2015).

[5]IMDb (2014): The Interview (2014), online unter: http://www.imdb.com/title/tt2788710/?ref_=nv_sr_1 (letzer Zugriff: 24.12.2014).

[6]Norton (2015): Bots and Botnets – A Growing Threat, online unter: http://us.norton.com/botnet/ (letzer Zugriff: 09.02.2015).

[7]Vangie Beal: DDoS attack – Distributed Denial of Service, online unter: http://www.webopedia.com/TERM/D/DDoS_attack.html (letzer Zugriff: 15.02.2015).

[8]Kushner, David (2013): The Real Story of Stuxnet, online unter: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (letzer Zugriff: 07.02.2015).

[9]Stingeder, Karl H. (2010): Case Study: North Korea. How predictable is the regime? Marburg: Tectum, 69–100 /Stingeder, Karl H. (2009): Die

Causa Nordkorea. Wie berechenbar ist das totalitäre und isolationistische Regime wirklich? Marburg: Tectum, 61–89.

[10]Vanityfair.com (2013): The Snowden Saga: A Shadowland of Secrets and Light, online unter: http://usnews.nbcnews.com/_news/2013/06/10/18882615-what-we-know-about-nsa-leaker-edward-snowden?lite (letzer Zugriff: 15.01.2015).

[11]IMDb (2015): WarGames 1983, published online: http://www.imdb.com/title/tt0086567/?ref_=fn_al_tt_1 (last viewed: 05.02.2015).

[12]Kushner, David (2013): The Real Story of Stuxnet, published online: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (last viewed: 07.02.2015).

[13]Vanityfair.com (2013): The Snowden Saga: A Shadowland of Secrets and Light, published online: http://usnews.nbcnews.com/_news/2013/06/10/18882615-what-we-know-about-nsa-leaker-edward-snowden?lite (last viewed: 15.01.2015).

[14]Time.com (2014): U.S. Sees North Korea as Culprit in Sony Hack, published online: http://time.com/3639237/sony-hack-north-korea-the-interview (last viewed: 15.02.2015).

[15]IMDb (2014): The Interview (2014), published online: http://www.imdb.com/title/tt2788710/?ref_=nv_sr_1 (last viewed: 24.12.2014).

[16]Norton (2015): Bots and Botnets – A Growing Threat, published online: http://us.norton.com/botnet/ (last viewed: 09.02.2015).

[17]Vangie Beal: DDoS attack – Distributed Denial of Service, published online: http://www.webopedia.com/TERM/D/DDoS_attack.html (last viewed: 15.02.2015).

[18]Kushner, David (2013): The Real Story of Stuxnet, published online: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (last viewed: 07.02.2015).

[19]Stingeder, Karl H. (2010): Case Study: North Korea. How predictable is the regime? Marburg: Tectum, 69–100 /Stingeder, Karl H. (2009): Die

Causa Nordkorea. Wie berechenbar ist das totalitäre und isolationistische Regime wirklich? Marburg: Tectum, 61–89.

[20]Vanityfair.com (2013): The Snowden Saga: A Shadowland of Secrets and Light, published online: http://usnews.nbcnews.com/_news/2013/06/10/18882615-what-we-know-about-nsa-leaker-edward-snowden?lite (last viewed: 15.01.2015).