Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 189 (2023)

Heft: 6

Buchbesprechung: Bücher

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 03.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

ROMANREZENSIONEN IN DER ASMZ?

Die ASMZ versteht sich als militärische Fachzeitschrift. Und deshalb ist es legitim, die Frage zu stellen, ob Romane bzw. Fiktion einen Platz unter den Rezensionen einer Fachzeitschrift haben. Wie an der nachstehenden Rezension gezeigt werden kann, gibt es verschiedene Gründe diese Frage – allerdings in Massen – zu bejahen: Romane erlauben mit Mitteln der Fiktion Szenarien über künftige Entwicklungen zu entwerfen und diese in ihren Konsequenzen «durchzuspielen», sie dienen mithin der Szenarienbildung. Erlauben Romane, so sie sich denn mit militärischen bzw. sicherheitspolitischen Themen auseinandersetzen, nicht nur eine Überprüfung der dem fiktiven Szenario zugrunde liegenden Annahmen und Prämissen, sondern erlauben damit auch eine weitergehende Auseinandersetzung mit den Grundlagen von Sicherheitspolitik. Aus diesem Grunde sollen in dieser und einer der folgenden Ausgaben exemplarisch Romane mit sehr unterschiedlichen Voraussetzungen und Szenarien vorgestellt werden, einer vom ehemaligen Schweizer Botschafter in den USA, Carlo Jagmetti, und der andere von Admiral James Stavridis (Co-Autor), dem ehemaligen Supreme Allied Commander Europe (SACEUR). *RSB*

Elliot Ackermann, Admiral James Stavridis

2034 – A Novel Of The Next World War

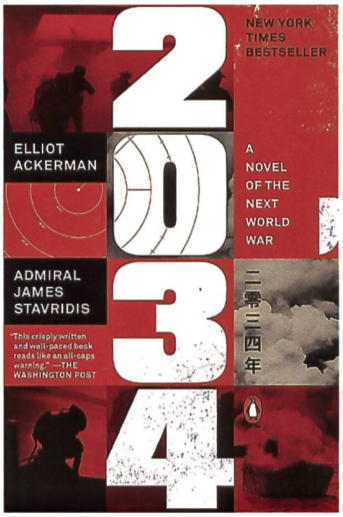
Der Krieg um die Ukraine hat die geopolitische Landschaft komplett verändert und frühere Szenarien über einen Dritten Weltkrieg sind obsolet geworden. So könnte man argumentieren und den 2021 in den USA veröffentlichten, aber bislang nicht ins Deutsche übersetzte Roman «2034 – A Novel Of The Next World War» unbeachtet lassen. Aber nichts wäre falscher als das. Es entginge dem Leser zunächst einmal die Lektüre eines gut geschriebenen Thrillers, aber weit mehr. Denn die beiden Autoren, Elliott Ackermann, ehemaliger Offizier der US-Marines und zeitweise im Weissen Haus tätig, und der pensionierte US-Admiral und ehemalige Supreme Allied Commander Europe der NATO (SACEUR) James Stavridis schildern einen amerikanisch-chinesischen Krieg höchst anschaulich. Hauptakteure sind nicht die Präsidentin der USA oder der Chef der kommunistischen Partei Chinas. Es sind eine Kommandantin der US Navy, ein US-Kampfpilot, ein Berater im Weissen Haus, ein Militärattaché an der chinesischen Botschaft in Washington und ein nach einer Generalmobilmachung im Iran reaktivierter General der Revolutionsgarden. Und alle erfüllen das, was sie als ihre Pflicht ansehen. Sie vertrauen dabei mehr auf ihre Intuition als auf die mehrfach versagende Technik. Unvermutete Cyber-Fähigkeiten und die gezielte Lähmung des Internets (u.a. durch die Zerstörung der transatlantischen Seekabel) sind

Game-Changer. Diese legen auf allen Seiten Informationssysteme der politischen und militärischen Führungszentren, Hightech-Waffen, die Stromversorgung und ganze Trägerverbände unerwartet lahm. Erschreckend real geschildert wird die Eskalationsdynamik von Provokation, Reaktion und Gegenreaktion usw. nach einem Zwischenfall im Südchinesischen Meer. Der Konflikt beginnt im März 2034 mit dem Abfeuern von Torpedos und Raketen, dem Versenken von Kriegsschiffen, führt fast nebenbei zur Einnahme von Taiwan durch die Volksrepublik China und endet im Juli 2034 mit dem Einsatz taktischer Nuklearwaffen und der Vernichtung ausgewählter Städte in den USA und China. Überraschend ist, wie und von wem dann der letzte Schritt zum Einsatz strategischer Nuklearwaffen und die gegenseitige Vernichtung doch noch verhindert werden. Doch dies sei hier nicht verraten.

Kritisch anzumerken ist, dass nur auf wenigen Seiten angedeutet wird, wie die Welt fünf Jahre nach diesem Krieg und nach mehreren Millionen Toten aussieht und welche geopolitischen Veränderungen stattgefunden haben. Dass die Handlung insgesamt nur auf eine Handvoll Personen konzentriert wird, ist ein typisch US-amerikanischer, eingängiger (und ggf. auch gut zu verfilmender) Topos, wonach das Schicksal der Welt in der Hand einzelner Individuen ruht. Sicherlich sind auch manche Charaktere und die politischen Systeme insbesondere in China und im Iran sehr einseitig gezeichnet. Aber das Buch wurde auch kaum mit dem Anspruch auf Objektivität oder den Literaturnobelpreis geschrieben.

Trotz dieser Schwächen lohnt die Lektüre aus mindestens drei Gründen: Angesichts der beruflichen Hintergründe beider Autoren liest sich erstens die Eskalationsdynamik erschreckend plausibel und das geschilderte Szenario ist eines, das geopolitisch und militärstrategisch Interessierte kennen und in eigene Überlegungen einbeziehen sollten. Zweitens wird deutlich aufgezeigt, welche unerwartete Dynamiken ein Krieg zwischen den USA und China auslösen könnte und wie andere Staaten als Trittbrettfahrer dann unkontrolliert ihre Interessen durchsetzen oder ihre Möglichkeiten nutzen. Und drittens spielen in diesem Buch 2034 weder die EU, und dies sollte angesichts des einen der beiden Autoren sehr zu denken geben, noch die NATO eine Rolle. Insofern sollte dies wiederum angesichts der Entwicklungen in Europa und der NATO seit dem russischen Angriff auf die Ukraine ein guter Grund sein, nach der spannenden Lektüre eigene Überlegungen darüber anzustellen, wie sich die Staaten in Europa und auch die NATO im Hinblick auf das Jahr 2034 und des absehbaren Wettstreits zwischen den USA und China positionieren sollten.

Oberst a.D. (GE)
Dipl. Päd. Reiner Haunreiter



New York: Penguin Press, 2021,
ISBN 9781984881267

IMPRESSUM

Nr. 6 – Juni 2023
189. Jahrgang

Präsident Kommission ASMZ
Oberst i Gst Thomas K. Hauser

Chefredaktor
Major a D Christian Brändli (cb)

Redaktionssekretariat
ASMZ c/o Verlag Equi-Media AG
Brunnenstrasse 7, CH-8604 Volketswil
Telefon +41 44 908 45 60
E-Mail: redaktion@asmz.ch
abo@asmz.ch

Stellvertretender Chefredaktor
Fachof Fritz Kälin (fk)

Redaktion
Oberst i Gst Michael Arnold, lic. phil. II (AM)
Oberst Dieter Kläy, Dr. phil. I (dk)
Oberstlt Pascal Kohler (pk)
Major i Gst Christoph Meier (cm)
Major a D Peter Müller, Dr. rer. pol. (pm)
Oblt Erdal Öztas (E. Ö.)
Hptm Daniel Ritschard, lic. oec. HSG (DR)
Oberst a D Bruno Russi (RSB)
Henrique Schneider (Sc)
Major Walter Troxler, Dr. phil. (Tr)
Oberstlt Hans Tschirren (HT)

Redaktionelle Mitarbeiter
Oblt Thomas Bachmann (tb)
Marc Ruef (mr)

Herausgeber
Schweizerische Offiziersgesellschaft

Verlag
Verlag Equi-Media AG,
Brunnenstrasse 7, CH-8604 Volketswil

Verleger
Christian Jaques

Geschäftsführer
Christoph Hämmig,
Telefon +41 44 908 45 60
E-Mail: haemmig@asmz.ch

Abonnemente
Silvia Riccio, Telefon +41 44 908 45 65
E-Mail: riccio@asmz.ch

Layout
Stefan Sonderegger

Inserateverkauf
Zürichsee Werbe AG
Eveline Schneider
Telefon +41 44 928 56 55
eveline.schneider@fachmedien.ch

Abo-Preis
inkl. 2,5% MwSt
Kollektivabonnement SOG ermässigt
Jahresabo Inland Fr. 78.– / Ausland Fr. 98.–
App-Jahresabo Fr. 67.–

Druck
pmc print media corporation,
CH-8618 Oetwil am See

Erscheinungsweise
11-mal pro Jahr

© Copyright
Nachdruck nur mit Bewilligung der Redaktion und Quellenangabe

www.asmz.ch

Member of the European Military Press Association (EMPA) – ISSN 0002-5925

Cyber-Security

Fachkräfte sind weltweit gefragt

Qualifizierte Fachkräfte für die Cybersicherheit zu finden, ist schwierig. Weltweit fehlen laut Schätzungen insgesamt über drei Millionen IT-Sicherheitsspezialisten. Mit dem neuen Bachelorstudium Cyber Security bildet die Fernfachhochschule Schweiz (FFHS) solche Fachkräfte aus.

Cybersicherheit gehört aktuell zu den grossen Herausforderungen in Industrie, Wirtschaft und Verwaltung. Bei einer Befragung der Universität Bern (2022) gaben rund 70 Unternehmen an, in den letzten beiden Jahren Ziel von Cyberangriffen geworden zu sein. Weltweit vergeht kein Tag, ohne dass ein Unternehmen gehackt, beraubt oder erpresst wird.

Diese Angriffe zielen nicht auf die IT-Systeme, wie Prof. Dr. Tobias Häberlein, Leiter des Departements Informatik an der FFHS, erklärt, sondern sehr häufig sind Menschen das Ziel. Konkret: menschliche Schwachpunkte werden von den Angreifern ausgenutzt. «Mitarbeitende sind wohl in Sachen Cybersicherheit die grösste Gefahr für Unternehmen. Schätzungen zufolge gehen 70 Prozent der Attacken auf ihr Konto. Sie werden beispielsweise Opfer von Phishing-Attacken», sagt Häberlein. Und die Angriffe würden in Zukunft noch raffinierter werden. So zum Beispiel durch Voice Cloning. Künftig wird eine kurze Stimmaufnahme einer Person ausreichen, um diese elektronisch mit beliebigem Inhalt zu imitieren. Eine intensive Schulung der Mitarbeitenden sei zwingend.

Hoher Praxisbezug

Was Unternehmen und Verwaltungen brauchen, sind qualifizierte Fachkräfte für Cybersicherheit. Warum gibt es weltweit einen so grossen Mangel an Spezialisten? Dazu Häberlein: «Es interessieren sich einfach zu wenige junge Menschen für technische Studiengänge.»

Hier will die FFHS ansetzen. Der neue Bachelorstudiengang Cyber Security zeichnet sich unter anderem durch den grossen Praxisbezug aus. Die Studierenden werden im Laufe des Studiums selbst zu Hackern. Und sie bekommen die Möglichkeit, ihr Können in verschiedenen Hackathons unter Beweis zu stellen. Strategische Kooperationen wie etwa mit der Schweizer Armee oder der ICT-Berufsbildung Schweiz sind geplant, sodass die Studierenden von zusätzlichem praxisnahem Know-how profitieren.

Der neue Studiengang ist gemäss Häberlein dennoch ein technisch ausgerichteter Bachelor, der gewisse Schnittstellen mit der Informatik hat, daneben spezifische Module rund um die Cybersicherheit beinhaltet. «Wir gehen in die Tiefe – unter anderem Kryptologie, IT-Forensik oder auch Secure Coding werden uns beschäftigen», erklärt Häberlein.

Positive Rückmeldungen

Der Fachkräftemangel schmerzt in erster Linie die Unternehmen. Heute ist es für Arbeitssuchende entscheidend, ob sie sich bei einem Unternehmen weiterbilden oder parallel ein Studium absolvieren können.

Wie alle Studiengänge bietet die FFHS auch diesen neuen Bachelorstudiengang im Blended-Learning-Modell an. Dabei werden 80 Prozent im begleiteten Selbststudium absolviert, 20 Prozent finden als Präsenzunterricht statt. «Jemand, der ein Studium berufsbegleitend schafft, kann nur hoch motiviert und gut organisiert sein», sagt Häberlein. Die Rückmeldungen der Unternehmen über das Studienmodell und das Zeitmanagement der studierenden Mitarbeitenden seien in den vergangenen Jahren jeweils positiv gewesen.

Weiterführende Informationen zum Bachelor Cyber Security finden Sie unter www.ffhs.ch

FFHS
Fernfachhochschule Schweiz
Mitglied der SUPSI

BSc Cyber Security

✓ Berufsbegleitend
✓ Persönlich
✓ Anerkannt

ffhs.ch/studium