2021/2/1: USA

DIE USA UND DIE INFORMATIONSKRIEGSFÜHRUNG

Digitale Kriege sind real und die Vereinigten Staaten sind ein Hauptziel. Angesichts der hybriden Angriffe zielen die Reaktionen da
Gegner abzuschrecken, aber auch direkte Maßnahmen zu ergreifen. Amerikanische „Soft Power“ in diesem Bereich ist eine Quell
Überlegenheit, aber auch der Zerbrechlichkeit, da die Instrumente eingesetzt werden, um denen entgegenzutreten, die sie entwor

Digitale Kriege erfordern die Bekräftigung der Souveränität der USA und ihrer westlichen Verbündeten und Partner im Cyberspace
Zeit, in der ihre (zivile und militärische) Infrastruktur bedroht ist. [2] Die Behauptung einer cyberoffensiven Haltung Amerikas ist Te
Abschreckungsstrategie gegen die wichtigsten gegnerischen Mächte (Russland, China, Iran, Nordkorea) und trägt bis zu einem ge
zur Beruhigung der Mittelmächte bei, deren Verteidigungsinfrastrukturen im Kontext hybrider Konflikte besonders ins Visier genom
[3]

Im Februar 2019 verkündete die Washington Post, wie in amerikanischen politischen Kreisen seit mehreren Monaten gehofft word
es dem amerikanischen Militär im Herbst 2018 gelungen sei, die Internet-Forschungsagentur in St. Petersburg „abzuschalten“ und
reibungslosen Ablauf der Zwischenwahlen in den Vereinigten Staaten zu schützen, indem es die Schädigung derjenigen verhinder
russische Einmischung in den Präsidentschaftswahlkampf 2016 befürwortet hätten. Dieser angebliche journalistische Knüller, über
internationalen Medien und sozialen Netzwerken ausführlich berichtet wurde, bestätigte ein seit mehreren Wochen in Washington
Gerücht über die Fähigkeit des Cyber Command der Vereinigten Staaten und der NSA der Trump Administration, „muskulöse“ Op
durchzuführen, um offensiv gegen mögliche Hacker vorzugehen, die mit dem Kreml in Verbindung stehen. Diese Operation war Te
„Interagency“ bezeichneten Bemühungen der gesamten amerikanischen Regierung, dem russischen Einfluss auf den Wahlprozes
entgegenzuwirken. Das Heimatschutzministerium (Department of Homeland Security), das Außenministerium, das Justizministeriu
FBI arbeiteten unter dem Kommando von General Paul Nakasone zusammen. Diese von Cybercom (dem zehnten gemeinsamen
seit 2018) geführte Einschüchterungsaktion erfolgte in Form einer digitalen Nachrichtenkampagne, die sich an mutmaßliche Hacke
um sie „davon abzubringen, sich durch Desinformation in den Wahlprozess einzumischen“.

Die „Informationskampagne“ im Zusammenhang mit dieser Gewaltdemonstration im Cyberspace spiegelte den Wunsch der US-Re
des US-Kongresses wider, die Einschüchterungs- und Abschreckungskapazität der Vereinigten Staaten im fünften Bereich des Ka
den Terrorismus zu vermitteln, der in der US-Doktrin genannt wird. Diese war daher Teil von STRATCOM und spiegelte die Entwic
öffentlichen Debatte über Informationsoperationen (Info Ops) und computergestützte Gegenmaßnahmen wider, die beide heute tra
Instrumente der psychologischen Kriegsführung für die amerikanische Doktrin sind. Seit einigen Jahren (2011-2019) sind diese De
transparenter geworden, wie man an den Anhörungen des Kongresses über die Offensivfähigkeit des US-Militärs im Cyberspace s

Die USA haben zwar die Informationskriege nicht verloren, aber sie haben dennoch ihren komparativen Vorteil bei der Kontrolle de
Informationsflüsse eingebüßt - die Verwundbarkeit ihrer digitalen Systeme im Falle einer politischen oder geopolitischen Krise wird
USA wurden in der Trump-Ära durch den „Bumerang-Effekt“ Opfer einiger Schlüsselelemente ihrer eigenen „Soft Power“. Ihre Fäh
Technologien zu schaffen, die die Nutzung digitaler Werkzeuge durch ihre Gegner fördern, ist zur Achillesferse ihrer Verteidigungs
geworden. Dementsprechend müssen die USA nun die nötigen Schritte unternehmen, um diese Schwachstellen auszumerzen. [4]

Russland und China als Herausforderer Amerikas, aber innerhalb ganz best Grenzen

Während sich die politischen Strategien Chinas [5] und Russlands in Bezug auf die Schutzverantwortung (Responsibility to Protec
ähneln, zeigen die beiden Länder nuancierte Unterschiede im Umgang mit spezifischen Notfällen. Beide bringen ihre Unterstützun
ersten beiden Säulen der R2P zum Ausdruck, wehren sich jedoch gegen Zwangsinterventionen unter ihrer Ägide, da sie die Sorge
innere politische Sicherheit und die Sorge um ihr internationales Image teilen. Nichtsdestotrotz sind russische Erklärungen in Fälle
syrischen Krise durchsetzungsfähiger und sogar aggressiver, während chinesische Erklärungen in der Regel vage und reaktiv sind
sich in diversen Studien zum Thema, dass der diplomatische Stil die russische und chinesische Wahrnehmung ihres eigenen Platz
sich entwickelnden internationalen Ordnung widerspiegelt. Die Erfahrungen der vergangenen Jahrzehnte schaffen für sie unterschi
Bezugspunkte und Statusperspektiven, was zu ihren unterschiedlichen Strategien bei der Signalisierung des Großmachtstatus füh
hinsichtlich seiner Aussichten auf einen Statusanstieg optimistisch ist, übt es mehr Selbstbeherrschung aus, um externe Eindämm
vermeiden und zögert, als unabhängiger „Spoiler“ aufzutreten. Unterdessen interpretiert Moskau seinen Großmachtstatus eher im
eines „Verlustes“ und ist daher geneigt, einen strengeren Ansatz zu wählen, um seinen Status zu signalisieren. Obwohl sich ihre p
Ausrichtungen bei vielen Gelegenheiten ergänzen, gibt es nichts, was mit einem chinesisch-russischen „Block“ vergleichbar wäre.

Russland reagiert sehr sensibel auf Ereignisse, die seinen Status in Frage stellen, und ist sehr risikobereit, wenn es darum geht,
wahrgenommenen Bedrohungen zu begegnen. Inmitten seiner anhaltenden Besorgnis darüber, in seiner traditionellen Einflusssph
gegenüber dem Westen „an Boden zu verlieren“, veranlasst Moskaus Risikoeinstellung es dazu, auf der internationalen Bühne die
lauten und sichtbaren Dissidenten zu spielen. R2P wurde ein Opfer dieses Ansatzes. Die R2P-Debatten bieten somit ein aufschlus
Prisma, durch das die Außenstrategien der beiden Länder analysiert werden können. Zusammenfassend lässt sich sagen, dass, o
beiden Regime instinktiv um gegenseitige Unterstützung bitten, um eine Isolierung im UNO-Sicherheitsrat zu vermeiden, Peking u
Fragen wie der Anwendung von R2P nicht die gleiche Perspektive haben.

Auf absehbare Zeit werden Moskau und Peking Washington als ihren gemeinsamen Hauptgegner betrachten und jeder wird den a
Hauptpartner behandeln. [6] Beide kennen jedoch auch sehr gut die Grenzen dessen, was der andere anbieten kann, da sie unter
Ziele und Agenden haben. [7] Während Russland sich vor einer zu großen Abhängigkeit von China abzugrenzen versucht, befürch
in unnötige Konflikte hineingezogen zu werden, die den friedlichen Aufstieg Chinas gefährden könnten.

Der weitere Erfolg dieser Partnerschaft hängt von der Fähigkeit beider Seiten ab, mit den zugrunde liegenden Differenzen umzuge
unterschiedliche Auffassungen von ihren eigenen Statusaussichten haben, stellt die vorübergehende Synergie zwischen den beid
den R2P-Debatten nicht unbedingt eine Norm für die Zukunft dar. [8]

Der neue US-Präsident Joe Biden dürfte die außen- und sicherheitspolitischen Grundkonstanten der Strategie seines Vorgängers
wahrscheinlich beibehalten und Russland [10] wie China [11] als Hauptbedrohungen und Konkurrenten wahrnehmen. [12]

Abgeschlossen: Anfa

Anmerkungen:

[1] Emilie Circé, „SHOOTING CYBER BULLETS - Framing cyberspace warfare into operations“. In: Marine Corps Gazette 11/2020

[2] Vgl. Joris Verbeurgt, „CYBERWARFARE IN EASTERN EUROPE“. In: European Security & Defence 10/2020, S. 82-87.

[3] Siehe etwa: Michael D. Schoenfeldt / Matthew L. Tyre / William Malcolm, „FIRE AND MANEUVER IN THE CYBERSPACE DOM
In: Cavalry & Armor Journal 3/2020, S. 14-21.

[4] Vgl. Toshi Yoshihara, „EVALUATING THE LOGIC AND METHODS OF CHINA’S UNITED FRONT WORK“. In: Orbis 2/2020, S.

[5] Avery Goldstein, „CHINA’S GRAND STRATEGY UNDER XI JINPING - Reassurance, Reform, and Resistance“. In: Internationa
/2020, S. 164-201.

[6] Joel R. Powers, „21ST CENTURY LEARNING“. In: Marine Corps Gazette 6/2020, S. 35-38.

[7] Siehe dazu etwa: Zheng Chen / Hang Yin, „CHINA AND RUSSIA IN R2P DEBATES AT THE UN SECURITY COUNCIL”. In: Int
Affairs 3/2020, S. 787-805.

[8] Stephen W. Miller, „DIRECT ASSAULT SUPPORT OF EXPEDITIONARY INTERVENTIONS - China and Russia Extend Their F
In: Military Technology – MT 6/2020, S. 19-22.

[9] Siehe etwa: Bruno Tertrais, „ENCORE UN SIÈCLE AMÉRICAIN? LES ATOUTS STRATÉGIQUES DES ÉTATS-UNIS FACE À
CONCURRENTS“.
In: Revue Défense Nationale 6/2020, S. 90-96.

[10] Céline Marangé, „LES DÉSACCORDS RUSSO-AMÉRICAINS SUR LA STABILITÉ STRATÉGIQUE ET LE CONTRÔLE DES
“.
In: Revue Défense Nationale 6/2020, S. 66-74.

[11] Michael Clarke / Jennifer S. Hunt / Matthew Sussex, „SHAPING THE POST-LIBERAL ORDER FROM WITHIN: CHINA’S INFL
INTERFERENCE OPERATIONS IN AUSTRALIA AND THE UNITED STATES“. In: Orbis 2/2020, S. 207-229.

[12] Vgl. Ryan D. Martinson, „DECIPHERING CHINA’S „WORLD-CLASS“ NAVAL AMBITIONS“. In: Naval Institute Proceedings 8/
54.

Weiterführende LINKS:

Secrets and Lies: Information Warfare During The Cold War and Today

THE CHINESE PEOPLE’S LIBERATION ARMY AND INFORMATION WARFARE

Russia's Information Warfare - Marine Corps University

THE NEXT PHASE OF RUSSIAN INFORMATION WARFARE

Russian Information Warfare: Lessons from Ukraine

Russian Information Warfare: Implications for Deterrence Theory

Strategic Information Warfare: A New Face of War | RAND

Information Warfare - Federation of American Scientists

THE UNITED STATES NEEDS AN INFORMATION WARFARE COMMAND: A HISTORICAL EXAMINATION

US Navy increases ceiling for Information Warfare Research Project

After ignoring warnings, the US struggles with China’s aggression

Growing concern over information warfare continues to shape military

America is losing the information war

Information Warfare in an Information Age

A Return to Information Warfare

U.S. MILITARY OPPORTUNITIES: INFORMATIONWARFARE CONCEPTS OF OPERATION

Beijing and Moscow join forces in ‘information war’ as China-US relations rapidly deteriorate

Chinese Concepts and Capabilities of Information Warfare

China’s information war