neralsekretär, sondern auch den Mitgliedsstaaten zugänglich zu machen. Informelle Diskussionen mit Experten von SHAPE könnten die Szenarioausarbeitung unterstützen. Zudem seien die NATO-Simulationen auf ihre Komplexitätstiefe und Realitätstreue zu prüfen und unter Einbindung der Minister der Mitgliedsstaaten durchzuführen. Letztere könnten zudem nationale „*Red Teams*" vorhalten, die im Krisenfall schnelle Entscheidungswege herstellen würden.

Das Frühwarnsystem könne optimiert werden, indem u. a. die Möglichkeiten moderner Kommunikation stärker ausgeschöpft würden. Zudem müssten auch Geschehnisse, die nicht eindeutig militärisch seien, berücksichtigt werden, um die Hybridität moderner Kriegsführung abzudecken.

Die Regeln zum Krisenfall, unter anderem im NATO *Crisis Management Handbook*, müssten letztlich dahingehend vereinfacht werden, dass sie verständlich und weitgehend interpretationsfrei seien. Zudem sollte dem Supreme Allied Commander Europe (SACEUR) die Befugnis erteilt werden, im Krisenfall ohne weitere Rücksprachen (allenfalls mit dem Generalsekretär) die NATO Response Force (NRF) zu mobilisieren und im NATO-Gebiet zu verlegen.

Die Autoren erkennen die Möglichkeit, dass die NATO als multilaterale Institution einem Einzelakteur in dessen Entscheidungsgeschwindigkeit wahrscheinlich immer unterliegen dürfte. Die von ihnen vorgeschlagenen Schritte würden dieses Defizit jedoch verringern. Es sei wichtig, dass ein potentieller Gegner von einer tatsächlichen Einsatzfähigkeit und Entscheidungsentschlossenheit der NATO auszugehen habe, einschließlich der Anwendung der nuklearen Mittel. Dadurch würden sowohl ihre Abschreckungsfähigkeit und ihre Möglichkeiten des Krisenmanagements, als auch das Vertrauen der Mitgliedsstaaten in die Allianz gestärkt.

https://www.globsec.org/wp-content/uploads/2017/05/GNAI-reanimating-natos-warfighting-mindset.pdf

Ted Piccone: Democracy and Cybersecurity. Brookings – Democracy and Security Dialogue Policy Brief Series. September 2017

Besprochen von **Dr. Christine Hegenbart**, Mitglied im Arbeitskreis „Junge Sicherheitspolitiker" der Bundesakademie für Sicherheit. E-Mail: christine.hegenbart@gmx.net

https://doi.org/10.1515/sirius-2018-0012

Öffentliche und private Informationen können über den Cyberraum manipuliert, gestohlen und missbraucht werden. Für demokratische Prozesse birgt dies große Gefahren. Die Politik muss daher reagieren und sicherheitspolitische Konsequenzen ziehen. In seinem Policy Brief beschreibt Ted Piccone im ersten Schritt drei Problembereiche – *Demokratische Wahlen, Menschenrechte* und *Internet Governance* –, in denen Cyber-Sicherheit besonderer Aufmerksamkeit bedarf. Im zweiten Schritt stellt er Handlungsempfehlungen vor, insbesondere für die *Community of Democracies*, für die die Studie verfasst wurde.

Die Problemdarstellung wird in drei Bereiche untergliedert.

(1) Demokratische Wahlen können über den Cyberraum auf verschiedene Arten manipuliert und gefälscht werden. Diesen Versuchen ist gemein, dass sie darauf abzielen, die öffentliche Unterstützung, die Legitimität und die Soft Power von Demokratien zu untergraben. Insbesondere autoritäre Regime wie China und Russland gelten als Urheber derartiger Cyber-Angriffe. Als Beispiele werden die *Leaks* im Vorfeld der US-Präsidentschaftswahlen 2015/2016 und die *Fake-News*-Kampagne kurz vor der Wahl in Frankreich 2016 genannt.

(2) Menschenrechte, wie die Meinungs- und Versammlungsfreiheit oder das Recht auf Privatsphäre, werden immer stärker mit Cyber-Mitteln angegriffen. Die digitalen Überwachungsmöglichkeiten haben so beispielsweise einen „‚chilling effect' on free speech". Auch setzen autoritäre Staaten im Namen der nationalen Sicherheit Zensurmaßnahmen und sogenannte *Internet Shutdowns* bzw. Sperrungen von Seiten sozialer Medien ein. Damit verhindern sie u. a., dass sich Nachrichten und deren Bewertungen verbreiten, so wie z. B. in der Türkei nach dem Putschversuch 2015.

(3) Internet Governance ist von besonderer Bedeutung für die Offenheit und die Sicherheit des digitalen Raums. Von seinem Ursprung her ist das Internet dezentral organisiert, basiert auf grenzüberschreitenden Informationsströmen und wird als ein Netzwerk von Netzwerken von privaten Akteuren betrieben. Diese Struktur, die seinen Nutzern viele Freiheiten bietet, wird immer stärker angegriffen. Vor allem China und Russland schränken zum einen auf nationaler Ebene den freien Zugang der Nutzer zum Internet ein; und zum anderen stellen sie auf internationaler Ebene die Art und Weise in Frage, wie die Interoperabilität des Internets gewährleistet wird. Sie wirken darauf hin, den *Multistakeholder*-Ansatz der *Internet Governance* durch einen „*state-centric multilateral approach*" zu ersetzen, damit staatliche Akteure größeren Einfluss erhalten.

Für diese drei Bereiche werden Handlungsempfehlungen gegeben:

(1) Im Bereich *Demokratische Wahlen* empfiehlt der Autor das Wahlsystem als Kritische Infrastruktur einzu-

stufen. Er gibt demokratischen Staaten fünf Empfehlungen: (a) den Wahlvorgang umfassend vor der Einflussnahme aus dem Cyberraum zu schützen; (b) die Öffentlichkeit durch Datentransparenz von der Integrität des Wahlprozesses zu überzeugen; (c) daran zu arbeiten, staatlich finanzierte oder patriotische Hacker aufzuspüren und zu bestrafen; (d) einen *Code of Conduct* zu entwickeln, der den Grundsatz der gegenseitigen Nichteinmischung in Wahlen festschreibt; und (e) internationalen Konsens herzustellen, dass ein willentlicher Angriff auf das Wahlsystem als physischer Angriff auf das staatliche Territorium einzustufen ist, welcher internationales Recht bricht und daher Maßnahmen des Selbstschutzes rechtfertigt.

(2) Im Bereich *Menschenrechte* hat es für den Autor höchste Priorität, dass demokratische Staaten mit positivem Beispiel vorangehen und Menschenrechte in der digitalen Welt respektieren. Daher sollen sie erstens daran arbeiten, angemessene Normen z. B. durch UN-Resolutionen, zu schaffen. Zweitens sollen Staaten bei Gesetzen und Regulierungen, die Inhalte im Web oder in der digitalen Kommunikation einschränken, stets die digitalen Menschenrechte berücksichtigen. Zudem nimmt Piccone Privatunternehmen in die Pflicht: Sie sollen Systeme, Produkte und Protokolle entwickeln, die Bürger vor fremden digitalen Zugriffen schützen.

(3) Im Bereich *Internet Governance* sieht Piccone die demokratischen Staaten verpflichtet, sich klar hinter dem Ziel einer offenen Internet Governance zu vereinen. Die *Community of Democracies* soll daher eine Cyber-Sicherheitsarbeitsgruppe einsetzen. Diese hat vier Aufgaben: (a) einen freiwilligen „*code of internet governance*" zu erarbeiten, der sich an bisherigen vielversprechenden Initiativen, wie der *Internet Governance Strategy 2016–19* des Europarates, orientiert; (b) die Ausbildung politischer Entscheidungsträger im komplexen Feld Demokratie und Cyber-Sicherheit zu koordinieren; (c) Mitgliedstaaten zu unterstützen, ihre Fähigkeiten zum Schutz der demokratischen Prozesse auszubauen; und (d) diese Fortschritte zu beobachten, zu begleiten und zu fördern.

Die vorliegende Studie gibt für die ersten beiden Problembereiche *Demokratische Wahlen* und *Menschenrechte* nur sehr allgemeine Empfehlungen. Erst für den dritten Bereich *Internet Governance* werden der *Community of Democracies*, dem eigentlichen Adressaten, konkrete Handlungsvorschläge unterbreitet.

https://www.brookings.edu/wp-content/uploads/2017/08/fp_20170905_democracy_cyber_security.pdf

Russlands Sondereinsatzkräfte

Sarah Fainberg: Russian Spetsnaz, Contractors and Volunteers in the Syrian Conflict, Institut français des relations internationales (IFRI), Russie, Nei. Visions, No. 105, 12. Dezember 2017

Tom Parfitt: President Putin's Private Army Pays a High Price for Syria Success, The Times (London), 30. Dezember 2017

Besprochen von **Dr. Hannes Adomeit**, Non-resident Fellow, Institut für Sicherheitspolitik an der Universität Kiel.
E-Mail: hannes.adomeit@t-online.de

https://doi.org/10.1515/sirius-2018-0013

Innerhalb weniger Wochen nach der Verkündigung des Einsatzes russischer Streitkräfte in Syrien am 30. September 2015 schaffte es Russland, das Kräfteverhältnis im Bürgerkriegsland zugunsten des Assad-Regimes zu verschieben. Nach rund zweieinhalb Jahren Krieg kontrollieren die syrischen Streitkräfte wieder den größten Teil des Landes. Dieser Erfolg aus der Sicht des Kremls konnte trotz des Einsatzes relativ begrenzter militärischer Ressourcen verbucht werden. Das russische Kontingent bestand aus nicht mehr 4.000 Soldaten und mehreren Dutzend Kampfflugzeugen, die von dem neu eingerichteten Luftwaffenstützpunkt in Hmeimim in der Provinz Latakia und der Marinebasis in Tartus aus operierten. Zudem wurden von strategische Bombenflugzeugen, Überwasserschiffen und U-Booten sowie vom ins östliche Mittelmeer zeitweise entsandten Flugzeugträger Admiral Kuznecov Angriffe gegen Ziele in Syrien durchgeführt.

Die Stationierung regulärer russischer Streitkräfte und ihrer Einsätze in Syrien sind vom Kreml nicht nur eingeräumt, sondern auch über seine Medieneinrichtungen wie Sputnik und RT propagandistisch hervorgehoben worden. Dies betrifft allerdings lediglich Luftschläge. Offiziell beteiligt sich Russland nicht an Bodeneinsätzen. In Wirklichkeit gibt es diese jedoch in Form der Anwendung vielfältiger neuer Militärkräfte, die an den syrischen Frontlinien neben den regulären Truppen eingesetzt worden sind.

Sarah Fainberg, Research Fellow am Institute for National Security Studies (INSS) in Tel Aviv, hat sich mit diesem wenig erforschten Aspekt der russischen Intervention in Syrien beschäftigt. Zu den im Konflikt offiziell verschwiegenen bewaffneten Kräften rechnet sie Sondereinheiten aus der seit 2013 einsatzbereiten integrierten Kommandostruktur Sondereinsatzkräfte der Streitkräfte der Russischen Föderation (SSO VS RF). Unterstellt wurden ihr die Sondereinsatzkräfte (*sily special'nych operacii*)