

Aufsatz

Sara Bazoobandi*

Der Informationskrieg des Irans

<https://doi.org/10.1515/sirius-2024-4002>

Kurzfassung: Der iranische Informationskrieg ist in den zurückliegenden Jahrzehnten allgegenwärtiger und komplexer geworden. Er besteht aus einer Kombination von Strategien, die die Kontrolle des digitalen Raums, der Medien und der Diaspora umfassen. Ziel ist es, Einflussoperationen zur Manipulation des globalen Narrativs und zur Begrenzung des Informationsflusses durchzuführen. Die iranische Regierung hat sowohl im In- als auch im Ausland massiv in ausgeklügelte Methoden und Instrumente zur Durchführung des Informationskriegs investiert. Inspiriert durch die politische Ideologie des Staates, insbesondere dem Konzept des „Sieges durch Angst“, setzt die Regierung menschliche Emotionen institutionell als Strategie der Abschreckung in ihrem Informationskrieg gegen die politischen Dissidenten innerhalb und außerhalb des Landes ein. Dieser Beitrag analysiert vielschichtige Strategien dieser Form der iranischen Kriegführung, die im internationalen Umfeld verfolgt werden.

Schlüsselwörter: Iran, Informationskrieg, soziale Medien, Naher Osten

Abstract: Iran's Information Warfare has become more pervasive and complex in recent decades. It is a combination of strategies that include controlling the digital space, media, and diaspora to conduct influence operations for manipulating the global narrative and limiting information flow. The Iranian government has been investing heavily both domestically and internationally in sophisticated methods and tools of conducting Information warfare Inspired by the political ideology of the state, particularly the concept of 'victory through fear', the government has institutionally used human emotions as a strategy of deterrence in its information war against the political dissidents inside and outside of the country. This article analyses multi-layered strategies of Iran's information warfare, which are pursued in the international environment.

Keywords: Iran, information warfare, social media, Middle East region

1 Einleitung

In der internationalen wissenschaftlichen Debatte zur Informationskriegführung wird viel über Russland und China gesprochen. Wenig bekannt ist, dass der Iran eine Form der Informationskriegführung praktiziert, die eigene Ziele, Strategien und Methoden enthält, die zu analysieren sich lohnt. Die iranische Regierung hat tatsächlich ein umfassendes und komplexes System der Informationskriegführung eingeführt. Dieses System verfolgt nach Innen den Zweck, den freien Zugang zu Informationen im Cyberbereich einzuschränken. Damit will die Führung des Irans Nachrichten kontrollieren – und zwar sowohl solche, die in den Iran gelangen als auch jene, die international über den Iran verbreitet werden. Auch geht es ihr darum, das globale Narrativ zu beeinflussen. Sie verfolgt in diesem Zusammenhang eine Reihe von Strategien, um die öffentliche Wahrnehmung Irans im Ausland zu manipulieren und damit Strategien ausländischer Staaten gegenüber dem Iran zu beeinflussen. Ein wesentlicher Teil der Informationskriegführung besteht in dem Versuch, die iranische Diaspora zu kontrollieren, zu unterdrücken und zu manipulieren. Etwa fünf Millionen Iranerinnen und Iraner leben außerhalb des Landes, viele von ihnen in Europa.¹ Daher nimmt die Kontrolle und Beeinflussung der Diaspora einen hohen Stellenwert in der Politik Teherans ein. Es lohnt sich folglich, die Dynamiken der Beziehungen zwischen der Diaspora und der Regierung in Teheran sowie zwischen Iranern, die im Ausland leben, und den Gastländern für die iranische Regierung in den Blick zu nehmen.

Eines der Schlüsselemente der iranischen Informationskriegführung besteht darin, politische Gegner und Rivalen sowohl im In- als auch im Ausland mit Desinformation unter Druck zu setzen. Ziel ist es, das eigene Regime zu schützen und dessen Macht (auf nationaler, regionaler

*Kontakt: Dr. Sara Bazoobandi, Wissenschaftliche Mitarbeiterin, GIGA – Leibniz Institut für Globale und Regionale Studien, Hamburg; E-Mail: Sara.Bazoobandi@giga-hamburg.de

1 Shirin Hakimzadeh: Iran: A Vast Diaspora Abroad and Millions of Refugees at Home, *Migration Policy Institute Webseite* (www.migration-policy.org), 1.9.2006.

und globaler Ebene) zu maximieren. Das bedeutet unter anderem, dass die iranische Regierung versucht, vor allem westliche Länder und deren Öffentlichkeit mit Fehlinformationen und sorgsam gestreuten Fehlinterpretationen seiner Politik zu versorgen.

Ein wichtiges Schlüsselement sind Strategien, mit denen im In- und Ausland politische Oppositionsgruppen destabilisiert oder zerschlagen werden sollen. Die Manipulation der westlichen Öffentlichkeit und politischen Entscheidungsträger zielt darauf ab, das globale Narrativ gegenüber der iranischen Regierung zu kontrollieren, Sympathisanten zu gewinnen und politische Entscheidungsträger in die Irre zu führen. Das geschieht durch Verfahren der Diskursmanipulation, des *Social Engineering* und der geschickten Propagierung der eigenen politischen Ideologie.

In diesem Beitrag werden verschiedene Aspekte der iranischen Informationskriegführung und vor allem die dort zur Anwendung kommenden divergierenden Methoden beleuchtet. Der Schwerpunkt des Artikels liegt auf der Analyse der wichtigsten Instrumente im Werkzeugkasten der Regierung. Den Ausgangspunkt bildet eine Darstellung der ideologischen Grundlagen und der politischen Entscheidungsfindung im Iran.

Der Artikel beginnt mit einer Definition von Informationskriegführung. Dem folgt ein Überblick über das Umfeld des Irans auf nationaler und internationaler Ebene, innerhalb dessen Informationskriegführung angesiedelt ist. Anschließend wird die Rolle der schiitischen Ideologie im Iran untersucht. In diesem Abschnitt wird das Konzept des „Sieges durch Angst“ als eines der einflussreichsten Konzepte in der politischen Ideologie der Regierung diskutiert. Die Analyse wird sich dann auf verschiedene, zum Teil seit Langem etablierte Strategien der iranischen Informationskriegführung konzentrieren: Institutionalisierung von Angst, Hacking-Angriffe, Nutzung von religiösen, kulturellen und Bildungszentren sowie Manipulation sozialer Medien und Diskurse. Dieser Beitrag befasst sich ausschließlich mit der internationalen Dimension der iranischen Informationskriegführung.

2 Definition von Informationskriegführung

Es gibt eine globale Debatte über die Definition von Informationskriegführung, bei der es leider keinen Konsens unter Experten über die exakte Begrifflichkeit gibt. Zumindest kann man davon ausgehen, dass ein Informationskrieg darauf abzielt, Ideen zu generieren, die Gruppen zusammenschweißen, um ein gemeinsames Ziel zu erreichen oder

aber genau diesen Prozess bei anderen zu unterbinden. Informationskriegführung kann zwischen Staaten oder zwischen Staaten und nichtstaatlichen Akteuren stattfinden. Menschen, Emotionen und Ideen spielen im Informationskrieg eine wichtige Rolle.

Informationskriegführung kann auf unterschiedliche Weise ausgetragen werden: durch Verzerrung und Zerstörung von Roh- und Digitaldaten oder von digitalen Signalen. Auch die Kontrolle physischer digitaler Infrastruktur gehört dazu, die der Eliminierung des physischen Zugangs zu Informationen (zum Beispiel Internetfilterung) dient. Aber sie kann auch im virtuellen Raum stattfinden: durch Online-, Print- oder Rundfunkinhalte, oder durch verschiedene Methoden der Wahrnehmungsmanipulation durch Agenten und Sympathisanten.

Das US-Verteidigungsministerium (DoD) definiert Informationskriegführung als den Einsatz informationsbezogener Fähigkeiten in Kombination mit anderen Operationsmitteln, um „die Entscheidungsfindung von Gegnern und potenziellen Gegnern zu beeinflussen, zu stören oder an sich zu reißen und gleichzeitig die eigenen zu schützen.“²

Informationskriegführung findet demnach in einem Umfeld statt, das aus „Individuen, Organisationen und Systemen, die Informationen sammeln, verarbeiten, verbreiten oder darauf reagieren“ besteht.³ Die Umgebung, in der der Informationskrieg stattfindet, wird dabei in drei Dimensionen unterteilt: physische, informative und kognitive. Die *physische* Dimension besteht aus den Befehls- und Kontrollsystemen des Gegners, den wichtigsten Entscheidungsträgern und der unterstützenden Infrastruktur. Die *Informationsdimension* besteht aus der Erfassung, Verarbeitung, Speicherung oder Verbreitung von Informationen durch den Angreifer und der Art und Weise, wie er diese Informationen schützt. Die *kognitive Dimension* umfasst Aktivitäten, die „den Geist derjenigen beeinflussen, die Informationen übermitteln, empfangen und darauf reagieren oder auf sie reagieren.“⁴

Aber innerhalb des Sicherheits- und Verteidigungsapparats der USA wird „Informationskriegführung“ auf unterschiedliche Weise definiert. Die United States Navy fasst Informationskriegführung rein quantitativ auf und konzentriert sich dabei auf datengesteuerte und technologiebasierte Fähigkeiten wie Kommunikation, Netzwerke, Nachrichtendienste, Ozeanographie, Meteorologie, Kryptologie, elektronische Kriegführung, Cyberspace-Operationen und Weltraum.⁵ Die Luftwaffe der Vereinigten

² United States Department of Defense 2012.

³ Ibid.

⁴ Ibid.

⁵ United States Navy 2020.

Tabelle 1: Ebenen und Dimensionen des iranischen Informationskriegs

	Physisch	Informativ und kognitiv
innenpolitisch	Beispiele: – Internet-Filterung, – Überwachung – körperliche Gewalt gegen Demonstranten, – Inhaftierung einflussreicher Oppositioneller,	Beispiele: – Aufrechterhaltung der Propaganda durch staatliche Medien, – Aufrechterhaltung der Ideologie durch religiöse Figuren, – psychologische Operationen zur Zeit des Aufstandes,
international	Beispiele: – Ermordung und Entführung von politischen Oppositionellen, – Nutzung von Religions-, Kultur- und Bildungszentren,	Beispiele: – Hackerangriffe, – Manipulation in den sozialen Medien, – Manipulation von Diskursen.

Staaten definiert es als militärische Fähigkeiten, die eingesetzt werden, um das menschliche Verhalten des Gegners absichtlich zu beeinflussen und mediale oder öffentliche Unterstützung während eines Konflikts hervorzurufen. Es erfasst verschiedene Aktivitäten, „von Worten und Bildern, die in den sozialen Medien gepostet werden, bis hin zur Präsenz eines bewaffneten Flugzeugs auf der Rampe“, die eine Botschaft der Sicherheit vermitteln und weder eine breitere Erzählung schaffen noch fördern können.⁶ Die Doktrin der Luftwaffe ist nicht ausschließlich auf den Menschen ausgerichtet. Es geht ihr um die Verfügbarkeit und Kontrolle von Daten. Aber sie beinhaltet auch den Versuch, die Ideen und Gedanken von Menschen zu beeinflussen. In dieser Doktrin wird Informationskriegführung zusammen mit verschiedenen anderen wirkungsbasierten operativen Ansätzen verwendet.

Die Nordatlantikpakt-Organisation (NATO) hat ein Konzept für den Einsatz von Soft Power, das jenem Teil der Doktrin der US-Luftwaffe ähnelt, die sich mit der Beeinflussung des Denkens von Menschen befasst. Sie definiert Soft Power als „die Fähigkeit, andere von den Zielen der NATO zu überzeugen oder zu ermutigen, einen alternativen Ansatz zu verfolgen, vor allem durch kulturelle und ideologische Mittel oder durch die Förderung von Nachahmung. In der NATO-Doktrin erfordert die Einführung von Soft Power eine „Kampagnenmentalität; klare, konsistente Kommunikationsstrategien und Wirksamkeitsmessungen; und ein entwickeltes Verständnis für das Zielpublikum und seine gesellschaftlichen Einstellungen und Kulturen.“⁷

Es gibt kein öffentlich zugängliches offizielles Dokument zur Doktrin der Informationskriegführung der iranischen Regierung. Dieser Aufsatz versucht zu rekonstruieren, wie die entsprechende Doktrin der iranischen Führung

aussehen könnte. Die Ausgangsvermutung ist, dass Informationskriegführung für die iranische Regierung mehrere Ebenen umfasst. In Tabelle 1 werden die verschiedenen Ebenen und Elemente der Informationskriegführung aus Sicht Teherans zusammengefasst. Wie einige der oben genannten Definitionen erfasst die iranische Informationskriegführung sowohl physische als auch informationelle und kognitive Bereiche. Sie wird im In- und Ausland durchgeführt. Die Instrumente und Methoden, die von der Regierung sowohl auf nationaler als auch auf internationaler Ebene eingesetzt werden, unterscheiden sich jedoch von denen, die beispielsweise von der NATO und den USA verwendet werden.

Einer der Hauptunterschiede zwischen der iranischen Doktrin der Informationskriegführung und derjenigen westlicher Regierungen beruht auf der spezifischen Bedrohungswahrnehmung des Regimes. Diese konzentriert sich auf politische Dissidenten. Der zunehmende politische Dissens im Iran, der sich in mehreren Runden weit verbreiteter Unruhen in den zurückliegenden Jahren widerspiegelte, wird von der Regierung als die größte Bedrohung für das Regime angesehen. Daher wird jede Form der politischen Opposition von der Regierung als feindselige Handlung eingestuft. Vor diesem Hintergrund hat die Regierung im Laufe der Zeit Strategien der Informationskriegführung gegen die Opposition und zivilgesellschaftlichen Aktivismus im Inland entwickelt.

Gelegentlich finden sich Hinweise in der offenen Literatur, die Rückschlüsse auf die Ziele und Instrumente des iranischen Regimes im Bereich der Informationskriegführung zulassen. Im Jahr 2016 wurde im Iran (auf Farsi) eine Studie veröffentlicht, die verschiedene Formen der Reaktionen auf städtische Aufstände untersuchte.⁸ Die Autoren arbeiteten an der Imam-Hussein-Universität, einer öffentlichen Universität, die mit dem Korps der Islamischen Re-

⁶ United States Air Force 2023.

⁷ NATO Standardization Office: Allied Joint Doctrine AJP-01, Brüssel 2022.

⁸ Amiri/Nafavi 2016.

volutionsgarden (IRGC) verbunden ist. Sie identifizierten 13 unterschiedliche Strategien zur Eindämmung städtischer Bürgeraufstände, darunter: die Verbreitung von Gerüchten über Infiltratoren unter den Demonstranten und die Darstellung der Forderungen der Demonstranten als obszön und irrelevant. Diese Studie war vermutlich nur eine von vielen staatlich geförderten Arbeiten über Strategien im Umgang mit inneren Unruhen. Sie bietet aber einen guten Einblick in die Beweggründe und die Auswahl der Instrumente der Regierung im Umgang mit der Opposition.

Irans Instrumentarium der Informationskriegführung hat sich im Laufe der Zeit durch die Zusammenarbeit verschiedener Institutionen entwickelt, von denen die ranghöchste das Büro des Obersten Führers ist. Diese Institutionen setzen sich aus zivilen, militärischen und akademischen Organisationen wie dem Außenministerium, dem Geheimdienstministerium, dem Innenministerium, dem IRGC und anderen Abteilungen innerhalb der Streitkräfte sowie ihren akademischen Mitgliedsorganisationen zusammen. Die Exekutiv- und Entscheidungsgewalt in allen iranischen Regierungsinstitutionen ist stark personalisiert, daher hängen ihre Strategien in erheblichem Maß von der Denkweise derjenigen ab, die diese Einrichtungen leiten. Es ist jedoch wichtig, sich vor Augen zu halten, dass nach der politischen Ideologie der iranischen Regierung der Oberste Führer des Landes das höchste politische Amt innehat und damit die mächtigste hochrangige politische Figur im Iran ist. Daher werden die Entscheidungen aller Regierungsorgane sowie die Ernennung von Entscheidungsträgern in wichtigen politischen Ämtern direkt und indirekt vom Amt des Obersten Führers kontrolliert. Die Entscheidungen des Obersten Führers werden in Absprache mit einem engen und loyalen inneren Kreis von Beratern getroffen, die diese Entscheidungen tatsächlich beeinflussen können. Gemäß dem ideologisch vorgegebenen Rahmen der Regierung unterliegen seine Entscheidungen keiner Überprüfung, da seine Befehle unter seinen treuen Anhängern als diejenigen Gottes angesehen werden.

Dieser Hinweis zeigt, dass die politische Ideologie der Regierung eine entscheidende Rolle bei der Informationskriegführung des iranischen Regimes spielt. Die frommen Anhänger dieser Ideologie sind seit der Islamischen Revolution 1979 bevorzugte Empfänger von staatlich verteilten finanziellen Vergünstigungen. Seit der Revolution ist ideologische Loyalität die wichtigste Voraussetzung für den Zugang zu den staatlichen Verteilungsmechanismen im Iran. Da die Regierung seit mehreren Jahrzehnten Zugang zu unerwarteten Ölgewinnen hat, kann sie im Austausch für ideologische und politische Loyalität erhebliche finanzielle Mittel verteilen. Diese Anreize wurden durch direkte finanzielle Unterstützung wie den Zugang zu Krediten,

staatlichen Zuschüssen, Beschaffungs- und Unterauftragsvereinbarungen sowie durch nichtfinanzielle Unterstützungsmechanismen wie den Zugang zu Hochschulbildung, Beschäftigungs- und Aufstiegsmöglichkeiten im staatlichen und halbstaatlichen Sektor sowie den Zugang zu bevorzugten Geschäftslizenzen verteilt. Diese bildet die Grundlage für die iranische Informationskriegführung.

3 Ideologie im Iran und die Erzeugung von Angst als Ziel der Informationskriegführung

Seit der Revolution hat die Ideologie für die iranische Regierung eine entscheidende Rolle bei der Ausbildung der Informationskriegführung gespielt. Im Rahmen der politischen Ideologie der Regierung ist der *Vali-e-Faghih* (das heißt der Oberste Führer der Islamischen Republik) der Führer einer globalen islamischen *Umma*. Seine Befehle, die die religiösen Pflichten seiner Anhänger definieren, müssen weltweit ausgeführt werden. Die politische Ideologie und der Diskurs der Regierung basieren auf der schiitischen Interpretation des Islam und dem messianischen Konzept der Rückkehr des zwölften schiitischen Imams (Imam Mahdi). Er wird als ein Retter wahrgenommen, der aus dem höheren Reich gesandt wurde und aus jahrhundertlangem Versteck zurückkehren wird, um die Menschheit zu retten. Gemäß der schiitischen Theologie wird der Mahdi aufsteigen, um ein globales islamisches Reich zu errichten.⁹ Unter konservativen iranischen schiitischen Geistlichen herrscht Konsens darüber, dass die Rückkehr des Erlösers und sein Sieg zur Etablierung seiner Weltregierung zunächst weithin umstritten sein und weltweit zu Turbulenzen und gewaltsamen Zusammenstößen führen wird. Laut schiitischen theologischen Quellen soll in dieser Phase Gewalt eingesetzt werden, um bei Gegnern große Angst hervorzurufen und diese zur Kapitulation veranlassen.¹⁰

In den zurückliegenden Jahrzehnten war zu beobachten, dass der *Mahdismus* einen hohen Stellenwert in der politischen Ideologie der Regierung eingenommen hat und in das Narrativ der Regierung und in dessen politische Strategie übernommen wurde. Kern dieses Narrativs ist es,

⁹ Kasra Arabi/Saeid Golkar: Iran's Revolutionary Guard and the Rising Cult of Mahdism: Missiles and Militias for the Apocalypse. *Middle East Institute Webseite*, 3.5.2022.

¹⁰ Ali Akbar Hosseini: (عج) مهدی حضرت سریع پیروزی عوامل [factors that facilitate the return of Imam Madi]. *Mouood Webseite*, <https://fa.mouood.com>, Oktober/November 2018.

den Obersten Führer, Ayatollah Khamenei, als eine politische Schlüsselfigur der schiitischen Welt darzustellen, die die Rückkehr des Mahdi ermögliche.¹¹ Dieser theologische Rahmen wurde auch verwendet, um das politische Konzept des „Sieges durch Angst“ (auf Arabisch: Nasr bel ro'ob) zu rechtfertigen, das seit der Islamischen Revolution in verschiedene Regierungsstrategien eingeflossen ist.¹² Hochrangige militärische und politische Persönlichkeiten im Iran bezeichneten dieses Konzept häufig als Begründung für Versuche der Regierung, Angst unter in- und ausländischen Gegnern zu erzeugen. Organisationen wie Amnesty International und Human Rights Watch haben die Sicherheitsinstitutionen im Iran wiederholt für grausame Akte physischer und psychischer Gewalt verurteilt, um diese Strategie zu verfolgen.¹³ Der UN-Berichtersteller für den Iran, Javaid Rehman, hat 2013 das Ausmaß der staatlich verordneten Gewalt im Iran als ähnlich dem von Verbrechen gegen die Menschlichkeit beschrieben.¹⁴ Es gibt Hinweise darauf, dass die Androhung von Gewalt gegen Oppositionelle in der Tat eine Schlüsselkomponente der iranischen Informationskriegführung ist.

„Sieg durch Angst“ ist tief in der politischen Ideologie der iranischen Regierung verwurzelt. Das Konzept basiert auf der menschlichen kognitiven Reaktion auf Angst und auf der Annahme, dass die Angst vor dem Feind ein emotionales Eingeständnis der Niederlage auslöst. Die Übernahme dieses Konzepts in Strategien staatlicher Institutionen im Iran wird hier als „Institutionalisierung der Angst“ bezeichnet. Der institutionelle Gebrauch von Angst ist tatsächlich ein integraler Bestandteil der iranischen Informationskriegführung. Angst ist ein bestimmender Faktor in den Beziehungen der Regierung zur Öffentlichkeit (sowohl auf nationaler als auch auf internationaler Ebene). Im Folgenden werden einige Beispiele aufgeführt, die erläutern, wie die iranische Regierung durch die Institutionalisierung von Angst durch Morde, Entführungen und erzwungene Geständnisse Informationskriegführung betreibt.

Mohammad Ali Abtahi, Stabschef des ehemaligen Präsidenten Khatami, verriet in einem Interview, dass seit der Revolution das Konzept des Sieges durch Angst zur Philosophie des konservativen politischen Lagers im Iran gehöre.¹⁵ Er wurde während des Aufstands im Iran 2009 verhaftet und inhaftiert, weil er das Wahlergebnis angezweifelt hatte. Seine Erfahrung mit psychologischer Folter im Gefängnis, die er als Werkzeug für sein erzwungenes Geständnis beschrieb¹⁶, ist ein beeindruckendes Beispiel für die Praxis der Institutionalisierung von Angst durch die iranische Regierung.

Nach den Aufständen im Iran im Jahr 2022 empfahl ein weiterer iranischer Theologe in einer staatlich geförderten Fernsehsendung, dass die Gegner der islamischen Regierung gemäß islamischen Texten öffentlich gefoltert werden sollten. Nur so könne die Angst vor Schmerzen und körperlicher Folter Proteste gegen die Regierung in Zukunft verhindern.¹⁷ Darüber hinaus bestätigen jüngste Berichte, dass iranische Staatsbürger, die im Jahr 2022 an regierungskritischen Protesten in Europa teilgenommen hatten, von den iranischen Behörden verhört wurden, wenn sie zurückreisten, um ihre Familien zu besuchen.¹⁸ Mehreren Berichten zufolge haben Sicherheitskräfte am Flughafen von Teheran elektronische Geräte und Pässe der Reisenden beschlagnahmt und ihnen während der Verhöre die Augen verbunden. Die größten Proteste gegen die Regierung außerhalb des Irans im Jahr 2022 fanden in Berlin statt und symbolisierten die Einheit der verschiedenen Fraktionen der Diaspora-Opposition. Berichten zufolge haben „Beobachter“ der iranischen Behörden vor allem Iraner ins Visier genommen, die an dieser Versammlung teilgenommen haben. Ziel ist es, die Menschen einzuschüchtern und Dissidenten davon abzuhalten, sich gemeinsam zu organisieren. Durch die Beobachtung und Belästigung iranischer Bürger im Ausland, die an regierungsfeindlichen Kundgebungen im Ausland teilnehmen, versucht die Regierung, innerhalb der iranischen Diaspora, ein Gefühl der Angst und Unsicherheit zu schüren.

Zur Institutionalisierung von Angst durch die Regierung gehören auch die Entführung und Ermordung von Oppositionellen im Ausland. Das Ziel solcher Aktivitäten ist es,

11 Ayatollah Mesbah Vali-e Faghih ra naye-bi Imam-i Zaman midanest [Ayatollah Mesbah, Considered Vali-e-Faghih as Imam Mahdi's substitute] www.hawzahnews.com, 1.1.2022.

12 Mani Parsa: tars va tars salari dar jomhoori-e eslami, proje-ie 'al Nasr bel Ro'b' [Fear and primacy of fear in the Islamic Republic, 'al Nasr bel Ro'b' project], *Radio Farda* 2022; <https://www.radiofarda.com/a/islamic-republic-tactic-of-fear/32164261.html>.

13 Iran: Internet deliberately shut down during November 2019 killings – new investigation, *Amnesty International, Press Release* 16.11.2020; siehe auch Iran – Events in 2021, *Webseite Human Rights Watch*, <https://www.hrw.org/world-report/2022/country-chapters/iran>.

14 Patrick Wintour: Iran rights violations amount to crime against humanity, says UN expert, *The Guardian*, 20.3.2023.

15 Donya-e-Eghtesad: Interview with Mohammad Ali Abtahi in: *Donya-e-Eghtesad*, <https://donya-e-eghtesad.com/>, 23.1.2023.

16 Ibid.

17 Abolfazl Bahrampour Comments on Channel 1. 2022. Directed by IRIB Channel 1. Available at: <https://www.youtube.com/abolfazl-bahrampour>.

18 Solmaz Ikdar, 2024. *فرونگاه در پاسپورت ضبط افزایش گذرنامه؛ اداره در بسته چشمان با بازجویی* [interrogated and blindfolded in the Passport Office: a rise in passport confiscation at the airport], <https://iranwire.com>, 6.1.2022.

oppositionelle Stimmen außerhalb des Landes physisch zu eliminieren. Die Regierung geht bei solchen Aktionen davon aus, dass eine führerlose Oppositionsbewegung in der Diaspora weniger Aussichten hat, die inneren Verhältnisse im Iran zu verändern. Schätzungen zufolge hat die iranische Regierung seit 1979 weltweit mehr als 360 Morde verübt.¹⁹ Im ersten Jahrzehnt nach der Revolution (1979–89) wurden solche Aktionen durch eine direkte Fatwa des Gründers der Islamischen Republik, Ayatollah Khomeini, angeordnet und von der Regierung als Bemühungen bezeichnet, „heilige Gerechtigkeit gegen Feinde der göttlichen islamischen Herrschaft“ in Teheran auszuüben.²⁰ In den zurückliegenden Jahren wurden Entführungsoperationen, Mordversuche und Geiselnahmen, die von Regierungsagenten und ihren ausländischen Sympathisanten durchgeführt wurden, nicht nur dazu benutzt, die iranische Diaspora und die Opposition im Exil zu unterdrücken, sondern auch, um Angst in der iranischen Diaspora, der ausländischen Öffentlichkeit und den politischen Entscheidungsträgern zu erzeugen. Damit sollte jede Form der politischen Opposition auf nationaler und globaler Ebene geschwächt werden.

Im Jahr 2019 wurde Rouhollah Zam, ein iranischer Journalist, der zu diesem Zeitpunkt in Frankreich lebte, von IRGC-Agenten im Irak verhaftet. Er betrieb von Paris aus einen sehr populären Telegram-Kanal (Amad News) auf Farsi, mithilfe dessen er Neuigkeiten und Skandale über verschiedene hochrangige iranische Politiker mitteilte. Seine Verhaftung wurde offenbar von den Revolutionsgarden geplant, die ihn in den Irak lockten. Die staatlich geförderten Medien im Iran berichteten über Zams Entführung im Irak in mehreren ausführlichen Fernsehberichten, in denen behauptet wurde, dass seine Entführungsoperation von der globalen und regionalen Gemeinschaft als Bestätigung des Mutes und der Macht der Revolutionsgarden interpretiert wurde.²¹

Ein weiteres Beispiel für den Einsatz von Angst in der iranischen Informationskriegführung ist ein vereitelter Bombenanschlag auf eine große Versammlung der Mujahedin-e-Khalq (MEK) in Frankreich. Die MEK ist eine iranische Oppositionsorganisation. Die französischen Behörden kamen zu dem Schluss, dass das iranische Geheimdienstministerium hinter dem Komplott steckte. Sechs Personen

wurden im Zusammenhang mit dem Komplott verhaftet, darunter ein hochrangiger iranischer Diplomat in Österreich.²² Letzterer war Chef des iranischen Geheimdienstnetzwerks in Europa.²³ Er wurde 2023 gegen europäische Gefangene ausgetauscht, die im Iran festgehalten wurden.²⁴ Das vereitelte Komplott des Irans wurde organisiert, um Angst in der Diaspora zu schüren, insbesondere unter den Anhängern der MEK.

Während jeder Runde der Volksaufstände im Iran berichteten persischsprachige Fernsehsender in der Diaspora ausführlich über die Ereignisse. Einer dieser Kanäle, der über die Proteste von 2022 und das gewaltsame Vorgehen der Regierung informierte, ist *Iran International*. Seitdem sind die Journalisten von *Iran International* verstärkt ins Visier der iranischen Regierung geraten. Teheran hat *Iran International* beschuldigt, von der saudi-arabischen Regierung bezahlt zu werden, um die Regierung im Iran zu schwächen. Auf verschiedenen Social-Media-Plattformen wurde eine heftige Verleumdungskampagne gestartet, um den Ruf derjenigen iranischen Journalisten zu beschädigen, die für den Sender arbeiteten. Online-Inhalte wurden von Millionen von Konten innerhalb und außerhalb des Irans erstellt, um die Mitarbeiter des Senders zu beleidigen und sie des Verrats an ihrem Heimatland zu beschuldigen. Auch wurden ihnen sezessionistische Tendenzen unterstellt. Viele riefen dazu auf, den Sender zu boykottieren. *Tasnim News*, eine Online-Nachrichtenagentur, von der bekannt ist, dass sie mit den Revolutionsgarden verbunden ist, hat zusammen mit verschiedenen anderen staatlichen iranischen Medienplattformen den Sender ins Visier genommen und insbesondere den Vorwurf des Separatismus verbreitet.²⁵

In London, wo sich der Hauptsitz von *Iran International* befindet, hatten Berichten zufolge iranische Regierungsvertreter im Jahr 2023 einem Menschenhändler 200.000 Dollar angeboten, sofern dieser zwei Nachrichtensprecher des Senders in ihren Häusern ermordete. Das Komplott wurde aber von der Person vereitelt, die die iranische Regierung angeheuert hatte. Der Mann teilte Details der Operation mit den britischen Medien. Ihm wurde unter anderem von den iranischen Agenten zu verstehen gegeben, dass er die beiden Sprecher „fertig machen“ müsse, um ein

19 Faramarz Davar: خمینی رانی حکم دوره: اسلامی جمهوری ترور و ربای آدم شمارگاه [Kidnapping and Terror by the Islamic Republic Under Khomenei], <https://iranwire.com/fa/features/54546/> (2021).

20 Faramarz Davar: ایران مرزهای از خارج در ترور برای دیگر تلاش یک آدم؛ های دیپلمات [Diplomat Assassins; More Effort for Assassination Outside of Iran], <https://iranwire.com/fa/features/54417/> (2021).

21 Zam's first hearing at the court in Iran [روح الله زم برگزاری اولین جلسه], BBC Persian, 10.2.2020.

22 Saeed Kamali Dehghan/Kim Willsher: France blames Iran for foiled bomb attack near Paris, *The Guardian*, 2.10.2018.

23 Jiyar Gol/Omid Montazeri: اسدالله: سه سال سه اسدی؛ اسدالله [Asadollah Assadi: three years of information war between Iran and the west], BBC Persian, 25.11.2020.

24 Charlotte Van Campenhout: Three more Europeans exchanged for Iran's Assadi in prisoner swap, *Reuters online*, 3.6.2023.

25 Tasnim News, 2022. روز ۲۰ در طلب جدایی چهره ۲۰ به تربیون / اینترنشنال آنتن [gathering of secessionists in Iran International]. www.tasnimnews.com/fa, 11.10.2022.

Exempel zu statuieren. Jeder im Sender solle wissen, was ihm blüht, wenn er gegen die iranische Regierung arbeitet.²⁶ Im März 2024 wurde dann doch ein weiterer Journalist von *Iran International* in der Nähe seines Wohnhauses von drei Männern niedergestochen. Die britische Anti-Terror-Polizei leitete eine Untersuchung des Anschlags ein, da sie auf eine Reihe von Drohungen gegen iranische Journalisten folgte.²⁷

4 Hackerangriffe als Instrument der Informationskriegführung

Offensive Cyberoperationen gehören ebenfalls zum Arsenal der iranischen Informationskriegführung. Es geht darum, entweder Informationen zu erhalten oder es wird versucht, vermeintlichen Feinden zu schaden. Seit über einem Jahrzehnt nutzt die Regierung in Teheran dazu eigene technische Kapazitäten oder sie weist Cyber-Proxys an und sponsert sie, um Hacking-Operationen in ihrem Auftrag durchzuführen. Die Regierung hat aufdringliche und zerstörerische bösartige Cyberaktivitäten organisiert, von denen oft behauptet wird, dass sie von einer Gruppe namens *Iranian Cyber Army* durchgeführt worden seien. Solche Aktivitäten haben seit dem Volksaufstand nach den umstrittenen Präsidentschaftswahlen von 2009 deutlich zugenommen.²⁸ Die Regierung des Irans hat massiv in technologische Fähigkeiten investiert, die für die Durchführung von Cyberangriffen im Iran und im Ausland erforderlich sind.

In den zurückliegenden Jahren hat die jährliche Gefährdungsanalyse der Geheimdienste der Vereinigten Staaten (US) die Ausweitung des iranischen Know-hows und die Zunahme der Bereitschaft zur Durchführung von Cyberoperationen als eine große Bedrohung für die Vereinigten Staaten und ihre Verbündeten bezeichnet. Die Cyberaktivitäten des Irans zielen darauf ab, ihre Fähigkeit zu demonstrieren, „in vielen Bereichen gegen die Vereinigten Staaten vorzugehen, und seine Bereitschaft, Länder mit stärkeren Fähigkeiten ins Visier zu nehmen.“²⁹

Der Iran verfolgt seit 2012 eine nationale Cyberstrategie, die in mehreren Schritten umgesetzt worden ist. Im Februar 2020 ordnete der Oberste Führer des Irans die Einrichtung des Obersten Nationalen Cyber-Weltraumrats an. Dieser wird vom Präsidenten des Landes geleitet und

soll die Nation vor dem schützen, was er als „potenzielle Schäden im Cyberbereich“ bezeichnete.³⁰ Der Rat koordiniert sich mit mehreren anderen Regierungsstellen, die gemeinsam die iranischen Cyber-Streitkräfte bilden. Dazu gehören das *Cyber Defence Command*, die *National Passive Defence Organisation* sowie die Cyberkräfte der *Basidsch* und der *Revolutionsgarden (IRGC)*. Es ist nicht bekannt, welches Segment dieser Organisationen die iranische Informationskriegführung im Ausland beaufsichtigt. Bekannt ist, dass die Regierung verschiedene Privatakteure angewiesen hat, „Computereinbrüche, Überweisungsbetrug und Datendiebstahl durchzuführen.“³¹

Irans Kapazitäten zur Cyberkriegführung haben sich in den zurückliegenden Jahren weiterentwickelt. Das liegt an den hohen Investitionen in diesem Bereich sowie an der Zusammenarbeit mit gleichgesinnten Staaten wie Russland³² und China.³³ Die Investitionen in die Informationskriegführung sind Teil der umfangreichen Förderprogramme der Regierung für den sogenannten „wissensbasierten“ Sektor. Dieser Begriff gehört zu den am häufigsten verwendeten Plattitüden des Obersten Führers des Landes und lässt erkennen, dass der Staat hier ein wichtiges Betätigungsfeld sieht.³⁴ Schon im Jahr 2014 gab er ein offizielles Kommuniqué heraus, das an alle Regierungsstellen im Iran verteilt wurde und die Politik in Bezug auf Wissenschaft und Technologie umriss.³⁵ Das Dokument enthält die Vision der Regierung für die wissenschaftliche Entwicklung des Irans. Dazu gehören unter anderem: ein ständiger wissenschaftlicher Dschihad (*Jahad-i Mostamar-i Elmi*), um die wissenschaftliche und technologische Position des Irans zu verbessern, den Iran zu einer wichtigen wissenschaftlichen Macht in der islamischen Welt zu machen und um iranische Talente zu identifizieren und zu fördern. Außerdem soll die Ausbildung an den Universitäten im Einklang mit dem islamischen Glauben erfolgen. Darüber hinaus gelte es bis März 2025 etwa vier Prozent des Bruttoinlandsprodukts (BIP) des Landes für die Verbesserung des wissensbasierten Sektors des Irans bereitzustellen.

30 Ayatollah Khamenei: شددن منصوب آن حقوقی و حقیقی اعضای و تشکیل مجازی [Supreme National Cyber Space Council is formed and its members are appointed], <https://www.leader.ir/fa/content/9213>, 14.9.2020.

31 Theohary 2020.

32 Council on Foreign Relations 2021.

33 Golnaz Esfandiari: Iran To Work With China To Create National Internet System, *Radio Free Europe/Radio Liberty*, 4.9.2020.

34 Bazoobandi 2023.

35 Ayatollah Khamenei, ۴ حداقل پژوهشیه بودجه افزایش / داخلی ناخالص تولید % [overall strategies for knowledge and technology development]. <https://www.leader.ir/fa/>, 20.9.2014.

26 Rohit Kachroo: 'The Wedding' – Iranian spy plot to kill two news presenters in London uncovered by double agent, *ITV News*, 21.12.2023.

27 Joshua Berlinger, Brutal stabbing of exiled Iranian journalist prompts counterterror investigation, *CNN*, 30.3.2024.

28 Anderson/Sadjadpour 2018.

29 Office of the Director of National Intelligence 2023.

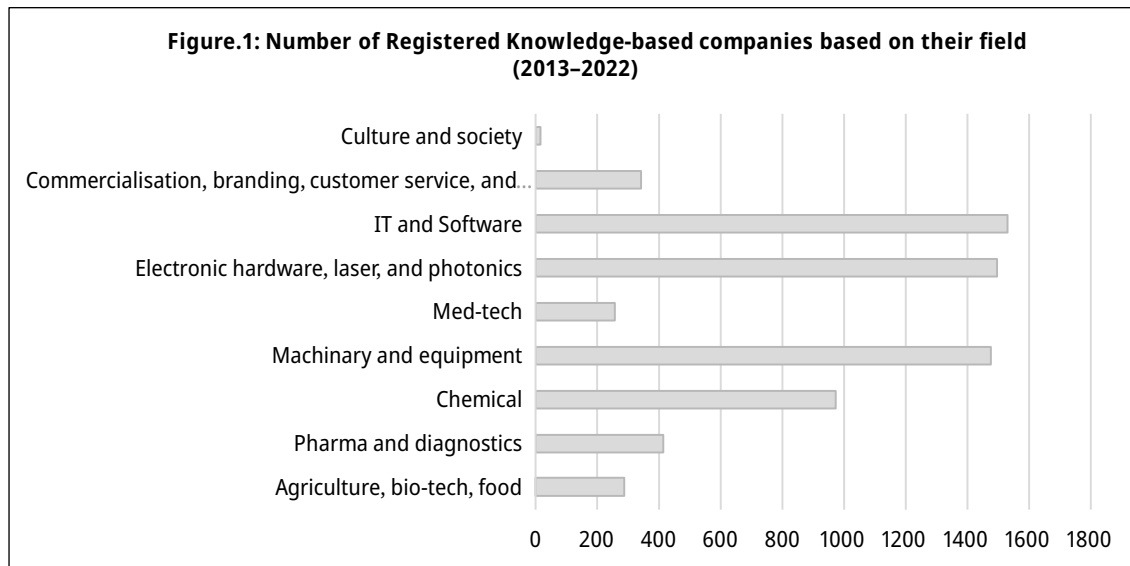


Abbildung 1: Anzahl der wissensbasierten Unternehmen unterschieden nach ihrem Feld der Expertise

Quelle: (isti.ir) بنیان دانش نمای داده | بنیان دانش موسسات و ها شرکت مرکز

Seit 2014 haben verschiedene offizielle Stellen neue Initiativen gestartet, um die Entwicklung des wissensbasierten Sektors im Iran zu verbessern.³⁶ Die Regierung hat in diesem Zusammenhang massiv in die Entwicklung von Cyber- und moderner Militärtechnologie sowie Kriegführung investiert. Der Oberste Rat für Wissenschaft, Forschung und Technologie, eine Regierungsbehörde, die direkt vom Büro des iranischen Präsidenten geleitet wird, veröffentlicht in Abständen Listen der wissensbasierten Güter und Dienstleistungen, die besonders gefördert werden.³⁷ Danach können sich Unternehmen auf den einschlägigen staatlichen Portalen für den wissensbasierten Sektor registrieren, um von den besonderen staatlichen Unterstützungsprogrammen zu profitieren. Wie aus Abbildung 1 hervorgeht, sind die meisten der auf dem Portal registrierten Unternehmen zwischen 2013 und 2022 an der Entwicklung von IT-Lösungen, Software, elektronischer Hardware, Lasertechnologie und Schwermaschinen beteiligt. Deutlich wird auch, dass sich die meisten Unternehmen, die in diesem Zeitraum im Iran als wissensbasierte Unternehmen registriert waren, an der Entwicklung von Cybertechnologien beteiligten. Solche Technologien werden häufig für internationales Hacking, Internetfilte-

rung und Überwachung eingesetzt. Darüber hinaus fallen einige andere militärische und verteidigungsbezogene Technologien wie Radargeräte und Funkkommunikation, die hauptsächlich im Militär eingesetzt werden, in die Kategorie „elektronische Hardware“.

Diese Kapazitäten wurden in den zurückliegenden Jahren für gezielte Cyberangriffe auf hochkarätige Aktivisten, Journalisten, Wissenschaftler und Karrierediplomaten genutzt, die sich mit dem Nahen Osten befassen. Im Jahr 2021 führte eine Gruppe namens APT42, auch bekannt als *Charming Kitten*, auf Anweisung der iranischen Regierung eine Reihe gezielter Angriffe auf mehrere Wissenschaftler weltweit durch. Die Gruppe kompromittierte eine echte Website, die der *School of Oriental and African Studies* der *University of London* gehört. Sie verschickten E-Mails, in denen behauptet wurde, von einem Mitarbeiter der Universität zu stammen, um Personen zur Teilnahme an einer Online-Konferenz einzuladen. Sobald der Austausch mit den Zielpersonen gesichert war, baten sie sie, ihre Teilnahme online über einen Link zu der kompromittierten Website zu registrieren. Die Cyberspione versuchten dann, über Telefone und Videokonferenzen eine Echtzeitverbindung zu Personen herzustellen.³⁸ Im Jahr 2022 berichtete *Human Rights Watch* über eine Reihe von Phishing-Angriffen, die ebenfalls von *Charming Kitten* durchgeführt wurden. Die Angriffe führten dazu, dass E-Mails und andere sensible

³⁶ Center for International Science and Technology Cooperation: Iranian VP: Knowledge-based firms best option to link universities to industrial sector. <https://cistc.ir/en>, 27.11.2022.

³⁷ Supreme Council of Science, Research and Technology, The list of knowledge-based goods and services [فهرست کالاها و خدمات دانش بنیان], <https://irkbn.com/>, Spring 2021.

³⁸ Gordon Corera: Iranian hackers posed as British-based academic, *BBC online*, 13.7.2021.

Daten zerstört oder kompromittiert wurden.³⁹ Im selben Jahr ließ der Iran einen zerstörerischen Cyberangriff gegen Einrichtungen der albanischen Regierung durchführen, die die iranische Oppositionsgruppe MEK in ihrem Land operieren lässt. Die Angriffe führten zum Abbruch der diplomatischen Beziehungen zwischen den beiden Ländern und zur Festnahme von iranischen Agenten, denen Spionage und Terrorismus im Auftrag der iranischen Regierung vorgeworfen wurde.⁴⁰

Vieles deutet darauf hin, dass die iranische Regierung massiv in inländische Cyberfähigkeiten investiert hat, während sie häufig mit externen Gruppen zusammenarbeitet, um weltweit Cyberoperationen durchzuführen. Das erschwert die Identifikation des Angreifers und seiner Hintermänner. Zudem weisen „private“ Akteure oftmals Fähigkeiten auf, die die Regierung oder die Revolutionsgarden noch nicht besitzen.⁴¹ Die iranische Regierung und die Revolutionsgarden werden weiterhin an der Ausweitung und Vervollkommenheit ihrer Cyberwar-Fähigkeiten arbeiten und dabei eng mit Russland und China kooperieren.

5 Die Nutzung von Religions-, Kultur- und Bildungszentren

Seit Jahrzehnten nutzt die iranische Regierung religiöse Zentren, um Informationen zu sammeln, Sympathisanten zu kooptieren und *Social-Engineering*-Operationen als Teil ihrer Informationskriegführung durchzuführen. Sie investiert in die Entwicklung eines Netzwerks von Angehörigen und Sympathisanten durch Aktivitäten verschiedener kultureller und religiöser Institutionen⁴² sowie von Bildungseinrichtungen auf der ganzen Welt.⁴³ Dieses Netzwerk hat das Ziel, die religiös-politische Ideologie der Regierung global zu verbreiten. Es gilt Menschen anzusprechen und zu Sympathisanten werden zu lassen, um die globale Agenda der iranischen Regierung voranzutreiben. Die Bemühungen der Regierung haben zwei Hauptvektoren: (1) die Macht des Westens, insbesondere der USA und ihrer Verbündeten,

weltweit zu untergraben; und (2) die eigene Macht und den eigenen Einfluss auf internationaler Ebene zu maximieren.

Diese Zielrichtung spiegelt sich im Mandat verschiedener iranischer transnationaler ideologischer und bildungspolitischer Projekte wider. Hier ist unter anderem die *Ahl-Beyt World Assembly* zu nennen, einer der größten sektiererisch-revolutionären parastaatlichen Akteure im Iran, die direkt dem Büro des Obersten Führers untersteht und von diesem kontrolliert wird. Die Mission der Organisation besteht darin, „der saudischen Version des Islam, die vom Westen unterstützt wird“, entgegenzutreten und den Muslimen der Welt den „reinen Islam“ vorzustellen.⁴⁴ In ähnlicher Weise fungiert die *Al-Mustafa Open University*, die Zweigstellen auf der ganzen Welt hat, auch in Deutschland und Großbritannien. Sie wird ebenfalls direkt vom Büro des Obersten Führers kontrolliert und stellt eine wichtige Institution zur Bildung und Erweiterung des religiösen und sektiererischen Netzwerks der Regierung auf der ganzen Welt dar und soll der Verbreitung der religiösen Staatsideologie dienen.⁴⁵

Eine besonders herausgehobene Rolle spielt in diesem Netzwerk das *Islamic Centre of England (ICE)*. Seit Jahren wird das Zentrum von Teheran genutzt, um die politische Ideologie der Regierung im Vereinigten Königreich zu verbreiten. Die ICE untersteht direkt dem Büro des Obersten Führers. Während der Aufstände im Iran im Jahr 2022 versuchte der ICE-Direktor, der direkt vom Obersten Führer ernannt wird, die legitimen pro-demokratischen Forderungen der iranischen Demonstranten in den Schmutz zu ziehen und bezeichnete sie als „Soldaten Satans.“⁴⁶

Im Jahr 2023 leitete die Wohltätigkeitskommission des Vereinigten Königreichs eine gesetzlich vorgeschriebene Untersuchung des Verhaltens der ICE ein, nachdem Bedenken hinsichtlich der Führung der Organisation und ihrer Verbindung zum Iran geltend gemacht worden waren. Im Januar 2024 leitete die britische Wohltätigkeitskommission eine weitere Untersuchung gegen die ICE ein, nachdem Videos von antisemitischen Reden iranischer Generäle aufgetaucht waren, die sie vor Studenten in Großbritannien gehalten hatten und in denen die Menge auf dem ICE-Gelände in London „Tod Israel“ skandierte. Die ICE hat auch eine öffentliche Mahnwache für Qassim Soleimani veranstaltet,

³⁹ Iran: State-Backed Hacking of Activists, Journalists, Politicians, *Human Rights Watch online*, 5.12.2022.

⁴⁰ Greta Zaimi: Iran's Balkan front – The roots and consequences of Iranian cyberattacks against Albania, Middle East Institute Webseite, 22.12.2022.

⁴¹ Freilich 2024.

⁴² Haruna Shehu Tangaza: Islamic Movement in Nigeria: The Iranian-inspired Shia group, *BBC online*, 5.8.2019.

⁴³ Gilda Sahebi/Jean-Philip Baeck: Kooperation mit Kaderschmiede, *taz-online*, 6.11.2023.

⁴⁴ Tolid-e Mohtava dar Fazay-e Majazi, Rahkar-e Moghabele ba Tahajom-e Farhangi-e Doshmanan-e Nezam ast [Our enemies' cultural offensive must be mitigated in cyberspace] IRNA-Presseagentur www.irna.ir, 19.3.2022.

⁴⁵ Siehe Banikamal/Ra'ees 2018.

⁴⁶ David Rose: Revealed – 'London office' of Iran terror Guards in heart of Jewish neighbourhood, *Jewish Chronicle online* www.thejc.com, 19.1.2023.

den Chef der Quds-Truppe der Revolutionsgarden (IRGC), nachdem dieser im Januar 2020 im Rahmen eines amerikanischen Luftangriffs getötet worden war. Soleimani war in den USA und Europa als Terrorist eingestuft worden.⁴⁷ Darüber hinaus haben Berichte enthüllt, dass seit dem 7. Oktober 2023 ein ausgeklügeltes Netzwerk iranischer Agenten die Pro-Palästina-Kundgebungen in Großbritannien anheizt.⁴⁸ In Anbetracht der Verbindungen der ICE zur iranischen Regierung und ihrer großen Netzwerke von Sympathisanten und Unterstützern in Großbritannien war sie wahrscheinlich an der Organisation von Pro-Palästina-Kundgebungen beteiligt, bei denen der Iran für seine Rolle in der Krise gelobt wurde. Die Wohltätigkeitskommission im Vereinigten Königreich hat jedoch keine offizielle Untersuchung zu diesem Vorwurf durchgeführt.

Der Iran fördert kulturelle und religiöse Projekte weltweit in der Absicht, damit politische Ziele zu verfolgen. Gerade die jüngsten Demonstrationen lassen erkennen, dass hierin ein Destabilisierungspotenzial besteht. Die meisten westlichen Regierungen haben sich bislang nicht dafür entschieden, Maßnahmen dagegen zu ergreifen.

Der Oberste Führer des Irans, der offiziell Oberbefehlshaber der iranischen Streitkräfte ist, einschließlich der IRGC, führt durch seinen Apparat auch direkt die religiösen Organisationen der Regierung im Ausland wie die ICE. Es ist daher sehr plausibel anzunehmen, dass kulturelle und religiöse Organisationen wie die ICE in der Verfolgung vorwiegend politischer Themen direkt oder indirekt mit den Agenten der Revolutionsgarden zusammenarbeiten. Das Mandat der ICE und anderer staatlich geförderter religiöser Zentren im Ausland umfasst allem Anschein nach ein breites Spektrum politischer Ziele. Dazu gehört die Legitimierung des Autoritarismus im Inland und das Sammeln von Unterstützung für vom Iran unterstützte Gruppen innerhalb der sogenannten „Achse des Widerstands.“

In den zurückliegenden Jahren wurden mehrere Attentate in Europa vereitelt. Untersuchungen verschiedener europäischer Sicherheitsbehörden haben ergeben, dass diese Operationen von den Revolutionsgarden gesponsert und koordiniert wurden. Zwischen 2020 und 2023 plante die iranische Regierung allein in Großbritannien 15 Tötungs- oder Entführungsoperationen. In Großbritannien war zu beobachten, dass lokale Vertreter der organisierten Kriminalität häufig angeheuert wurden, um Entführungen,

Zwangsrückführungen und die Ermordung von Gegnern der iranischen Regierung durchzuführen.⁴⁹ Die mögliche Verbindung zwischen den kulturellen und religiösen Zentren der iranischen Regierung mit solchen Anschlägen ist eigentlich bekannt, wird aber kaum von Sicherheitsbehörden in Europa aktiv bekämpft.

Auch das Islamische Zentrum in Hamburg hat Soleimani von den Revolutionsgarden offen unterstützt und Gedenkgottesdienste für ihn gesponsert. Darüber hinaus organisiert das Zentrum seit einigen Jahren Kundgebungen zum Al-Quds-Tag in Berlin. Dabei handelt es sich um den letzten Freitag des Fastenmonats Ramadan. Er wurde vom Gründer der Islamischen Republik, Ayatollah Khomeini, als Mahnung für das Engagement des Irans zur Zerstörung Israels benannt.⁵⁰ Solche Aktivitäten wurden bislang von der Bundesregierung eher dilatorisch behandelt, möglicherweise, um die diplomatischen Kontakte zu Teheran nicht zu stören. Seit dem 7. Oktober 2023 gibt es jedoch deutliche Hinweise in Richtung einer strengeren Überwachung der Aktivitäten dieser Organisationen in Deutschland. Im November 2023 führte die deutsche Polizei im Rahmen einer Untersuchung gegen das Islamische Zentrum Hamburg wegen seiner Verbindungen zur iranischen Regierung und zur libanesischen Hisbollah eine groß angelegte Untersuchung an mehr als fünfzig Orten im ganzen Land durch.⁵¹

Die Aktivitäten der vom Iran gesponserten kulturellen und religiösen Zentren unterliegen einer klaren strategischen Planung der iranischen Regierung. Diese religiösen und pädagogischen Initiativen dienen dazu, langfristige politische Ziele der iranischen Informationskriegführung zu verfolgen. Der ideologische Rahmen der Regierung und die Zuweisung erheblicher finanzieller Ressourcen bilden den Rahmen, innerhalb dessen diese Aktivitäten beurteilt werden müssen.

6 Einflussoperationen über soziale Medien

Soziale Medien sind weltweit zu einem wichtigen Bestandteil von Informationskriegführung geworden. Staatliche und nichtstaatliche Akteure nutzen unterschiedliche Social-Media-Plattformen, um ihr Narrativ zu verbreiten, an die Öffentlichkeit zu appellieren, Sympathisanten und Agenten

⁴⁷ Robert Mendick: UK-registered Islamic charity has described Qasim Soleimani as a 'great martyr,' *The Telegraph* 6.1.2020.

⁴⁸ Charles Hymas: Pro-Palestine protests in UK, stirred up by Iranian and Hamas network, *The Telegraph*, 19.10.2023, siehe auch Fiona Hamilton/Charlie Parker/Matt Dathan: Iran is hijacking UK pro-Palestinian protests, police warn. *The Times online*, 27.10.2023.

⁴⁹ Dominic Casciani: Hostile-state threat probes grown fourfold – police, *BBC online*, 16.2.2023.

⁵⁰ Cohen 2022.

⁵¹ German police raid Islamic centre over alleged ties to Iran, *Hezbollah, Al Jazeera online*, 16.11.2023.

zu rekrutieren oder Ereignisse zu manipulieren. Staatliche und nichtstaatliche Akteure haben über soziale Medien divergierende Formen des *Social Engineering* durchgeführt: Sie wenden zentral geplante Strategien an, um politische Stimmung zu machen, Wahlen zu beeinflussen und vor allem den demokratischen Konsens in westlichen Gesellschaften zu zerstören. Die iranische Regierung hat die sozialen Medien aktiv genutzt, um solche Ziele inner- und außerhalb des Landes voranzutreiben. Die Manipulation durch soziale Medien ist Teil der Cyber-gestützten Einflussoperationen des Irans und ihrer Informationskriegführung.

Irans *Social-Media*-Operationen verfolgen im Großen und Ganzen vier Ziele: (1) Destabilisierung westlicher Gesellschaften und oppositioneller Kräfte, (2) Vergeltung, (3) Einschüchterung und (4) Untergrabung der internationalen Unterstützung ihrer Gegner. Es geht darum, allgemeine Verwirrung und Misstrauen zwischen Gegnern und deren Verbündeten zu schaffen.⁵² Diese Ziele werden im Iran häufig durch den Einsatz unterschiedlicher Methoden verfolgt: So werden massenweise falsche digitale Identitäten aufgebaut (Sockenpuppen), um weitgehende gesellschaftliche Unterstützung für politische Ziele der Regierung in Teheran zu suggerieren. Indem falsche Behauptungen immer wieder durch eine Vielzahl von „gefakten“ Adressen verbreitet und bestätigt werden, sollen sich die Narrative der Regierung verstärken. Manche bezeichnen dieses Vorgehen als Taktik der verbrannten Erde.⁵³

Die iranische Regierung hat massiv in den Auf- und Ausbau eines Netzwerks von Cyber-Agenten mit verschiedenen ausgeklügelten technischen Fähigkeiten investiert, die in unterschiedlichen Phasen ihrer Informationskriegführung eingesetzt werden. Eine der Schlüsselstrategien Irans bei der Nutzung sozialer Medien bestand zum Beispiel darin, überzeugende Persönlichkeiten auftreten zu lassen, die sich als Freunde und Gegner der Regierung tarnen. Solche Techniken wurden während des Aufstands im Iran im Jahr 2022 häufig eingesetzt, um die Oppositionsgruppen zu verunsichern. Die gleiche Methode wurde nach dem Krieg gegen Israel am 7. Oktober 2023 angewandt. Die iranischen Cyber-Agenten haben Berichten zufolge gezielte Inhalte erstellt, die darauf gerichtet sind, die Soldaten der Israelischen Verteidigungskräfte (IDF) davon zu überzeugen, den Krieg aufzugeben und nach Hause zurückzukehren. Der Kern der Kampagne war die Behauptung, dass die IDF nicht in der Lage seien, ihre eigenen Soldaten zu schützen. Ein weiteres Beispiel nach dem 7. Oktober 2023 war die von iranischen Agenten durchgeführte Operation, die

als „Tränen des Krieges“ bezeichnet wurde. Ihr Ziel war es, Israelis davon zu überzeugen, sich in ihrem eigenen Land einer Kampagne zur Absetzung des israelischen Premierministers Netanjahu anzuschließen.⁵⁴

Außerdem bemüht sich der Iran, nach dem Vorbild Chinas und auch Russlands Online-Inhalte im eigenen Herrschaftsbereich zu kontrollieren und bei Bedarf zu löschen. Zu diesem Zweck wurden verschiedene Überwachungs- und Filterinstrumente eingeführt. Diese Methoden beschränken sich nicht nur auf den Iran selber. Während der Aufstände im Jahr 2022 hat die Regierung offenbar ein Netzwerk von Partnern und Agenten genutzt, um *Social-Media*-Inhalte außerhalb des Irans zu regulieren.

Meta, der Eigentümer einiger der am weitesten verbreiteten *Social-Media*-Plattformen der Welt (wie Instagram oder Facebook), hat seine Content-Moderation an verschiedene Unternehmen weltweit ausgelagert. Eines dieser Unternehmen ist *Telus International* mit Hauptsitz in Dublin und einem zweiten Büro in Essen. *Telus* beschäftigt unterschiedlichen Berichten zufolge etwa 500 Mitarbeiter in seiner Farsi-Sprachabteilung. Die meisten von ihnen sind laut den Whistleblowern iranische Studenten aus Europa, die häufig in den Iran reisen.⁵⁵ Im Jahr 2022 behaupteten Whistleblower, dass die iranische Regierung vielen von ihnen zwischen 5.000 und 10.000 Euro angeboten habe, um missliebige Inhalte zu löschen und um Konten zu zensurieren, die aktiv an der Dokumentation und Berichterstattung über die gewaltsame Unterdrückung von Protesten durch die Regierung im Jahr 2022 beteiligt waren.⁵⁶ Ein iranischer Mitarbeiter von *Telus* berichtete *BBC Persian*, dass einige der Mitarbeiter ihre persönlichen Mobiltelefone vor Ort und in ihrer Pause benutzten, um Konten wegen unangemessener Inhalte an iranische Vertrauenspersonen zu melden. Nachdem sie später an ihren Schreibtisch zurückkamen, haben sie die entsprechenden Posts entfernt oder Konten gesperrt.⁵⁷ Darüber hinaus wurde *Meta* von iranischen Oppositionellen beschuldigt, dass seine Messaging-Plattform mit der Regierung des Irans kooperiert habe in der Absicht, die Kommunikation iranischer Nutzer in der Diaspora zu stören.⁵⁸ *Meta* hat all diese Vorwürfe zurückgewiesen. Ver-

⁵² Microsoft Threat Intelligence 2024.

⁵³ The Scorched-Earth Tactics of Iran's Cyber Army, *Wired-online* (www.wired.com), 21.3.2023.

⁵⁴ Microsoft Threat Intelligence 2024.

⁵⁵ Parham Ghobadi: Instagram moderators say Iran offered them bribes to remove accounts, *BBC online*, 27.5.2022.

⁵⁶ Adam Kredo: Congress Wants To Know Why Meta Is Censoring Iranian Dissidents, *Washington Free Beacon online* (<https://freebeacon.com>), 7.6.2022.

⁵⁷ یا حکومت ایران در اینستاگرام نفوذ کرده است؟ [Has Iranian government penetrated Instagram?], *BBC Persian*, 17.5.2022.

⁵⁸ Meta Denies Accusations That It's Working With Iranian Government To Disrupt WhatsApp, *Radio Free Europe/Radio Liberty-online*, 23.9.2022.

treter des Unternehmens sagten, dass das Unternehmen eine große Anzahl von Mitarbeitern beschäftigt, die Inhalte in 70 Sprachen überwachen, und dass sie klare Anweisungen haben, nur das zu entfernen, was als Verstoß gegen die Unternehmensrichtlinien angesehen wird.⁵⁹

Im Juni 2022 leitete der US-Kongress allerdings eine Untersuchung gegen *Meta* wegen Zensur iranischer Dissidenten ein.⁶⁰ Der Kongress interessierte sich insbesondere dafür, welche Schritte das Unternehmen unternommen habe, um der Infiltration durch Befürworter des iranischen Regimes entgegenzutreten. Anlass dafür waren die oben erwähnten Berichte, wonach Moderatoren von Instagram-Inhalten Konten gelöscht und zensiert hätten, die das gewaltsame Vorgehen der Regierung während der Proteste im Jahr 2022 dokumentierten. Zu den gelöschten Inhalten gehörten Videos von Demonstranten, die Slogans wie „Tod für Khamenei“ skandierten, oder solche, die dokumentierten, wie iranische Sicherheitskräfte Tränengas auf Demonstranten abfeuerten.⁶¹ Es ist erwähnenswert, dass *Telus International* inzwischen auch von der russischen Opposition beschuldigt wurde, Inhalte in russischer Sprache zu zensieren und die Propaganda der Regierung in anderen Sprachen wie Bulgarisch zu fördern.⁶²

Die Manipulation der sozialen Medien ist ein weit verbreitetes und häufig genutztes Instrument im Werkzeugkasten der iranischen Informationskriegführung. Cyber-gestützte Einflussoperationen des Irans über soziale Medien nach großen globalen Ereignissen oder innenpolitischen Krisen haben deutlich zugenommen. Diese Operationen zielen auf Krisenbewältigung ab. Aber es gibt auch präventive Verfahren, die danach streben, die Ergebnisse künftiger Ereignisse zu manipulieren. Es wird erwartet, dass Beeinflussungsoperationen in naher Zukunft zunehmen werden. Es muss davon ausgegangen werden, dass auch die US-Wahlen im November 2024 vom Iran beeinflusst werden. Dies stellt eine Herausforderung für die demokratischen Prozesse in den USA und darüber hinaus dar. Man muss davon ausgehen, dass das Bedrohungsumfeld, das durch die iranische Informationskriegführung geschaffen wird, in den kommenden Jahren weiter zunehmen wird.

7 Manipulation von Diskursen

Ein weiteres Element der iranischen Informationskriegführung besteht in der Manipulation globaler politischer Diskurse. In den zurückliegenden zwei Jahrzehnten konzentrierte sich die politische Aufmerksamkeit westlicher Regierungen hauptsächlich auf das Atomprogramm Irans. In diesem Zusammenhang hat Teheran verschiedene Formen der Diskursmanipulation eingesetzt. Ein typisches Beispiel dafür ist die Behauptung, dass die schwierige wirtschaftliche Lage des Irans durch die Wirtschaftssanktionen der USA entstanden seien. Tatsächlich ist die wirtschaftliche Lage des Irans durch die Sanktionen verschärft worden. Aber letztlich waren und sind es andere Faktoren, die den Niedergang der wirtschaftlichen Lage des Irans bewirkt haben. Ein wichtiger Faktor sind die extrem hohen Ausgaben für die innere Sicherheit und für die militärische Rüstung – sowohl für das eigene Militär, die Pasdaran und nicht zuletzt die vielen Milizen und militanten sowie terroristischen Bewegungen, die der Iran im Nahen Osten unterhält. Diese Fehlallokation hat entscheidend zur Verschlechterung der wirtschaftlichen Lage des Landes beigetragen. Des Weiteren haben Korruption, betrügerische Finanzaktivitäten und die Veruntreuung öffentlicher Gelder, die durch Missmanagement in den Regierungsbehörden im Iran verursacht werden, eine wichtige Rolle bei der wirtschaftlichen Not im Iran gespielt. Man muss heute davon ausgehen, dass in den zurückliegenden Jahrzehnten große Summen an öffentlichem Eigentum von Regierungsmitgliedern gestohlen wurden.⁶³ Aber die Regierungsvertreter und ihre Sympathisanten haben das globale Narrativ über den Iran manipuliert, um alle sozioökonomischen Herausforderungen allein auf die Sanktionen zu schieben.

Im Jahr 2021 hat die Regierung die Militärausgaben um 11 Prozent (im Vergleich zum Vorjahr) auf 24,6 Milliarden US-Dollar erhöht. Der Iran gehört heute zu den 15 Ländern mit den höchsten Militärausgaben der Welt. Es ist erwähnenswert, dass das Budget der Revolutionsgarden im selben Jahr 34 Prozent der gesamten Militärausgaben des Landes ausmachte und um 14 Prozent anstieg.⁶⁴ In Verbindung mit Korruption auf hoher politischer Ebene in verschiedenen Regierungsorganisationen hat dies zur Verschlechterung der wirtschaftlichen Bedingungen im Iran beigetragen.⁶⁵

⁵⁹ Siehe Fußnote 57.

⁶⁰ Adam Kredo, a.a.O.

⁶¹ Iran International: Instagram is removing Iran International's videos of Iranian security forces firing tear gas at protesters. *Twitter.com* 12.5.2022; https://twitter.com/IranIntl_En/status/1524861794359164938.

⁶² Atanas Tchobanov: Meta, Telus, Censorship and Pro-Russian Propaganda. *Bird.bg-online*, 18.1.2023.

⁶³ Corruption and Mismanagement Index. *United Against Nuclear Iran Webseite*, <https://www.unitedagainstnucleariran.com/corruption>.

⁶⁴ Stockholm International Peace Research Institute (SIPRI): Trends in World Military Expenditure, 2021, https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf.

⁶⁵ Danielle Pletka: Corruption Is the Iranian Regime's Achilles' Heel, *Foreign Policy online*, 28.2.2023.

Der Diskurs der iranischen Regierung ist jedoch darauf ausgerichtet, die USA und die Sanktionen als den einzigen Grund für die wirtschaftliche Not des Landes darzustellen. Im Jahr 2019 erklärte der Oberste Führer des Irans in einer Rede, dass die Sanktionen dem Land zwar wirtschaftliche Schwierigkeiten bereitet, die politischen Entscheidungsträger aber dazu veranlasst hätten, ihre Ressourcen strategisch einzusetzen.⁶⁶ Während der globalen Covid-19-Pandemie behauptete der ehemalige Außenminister Mohammad Javad Zarif, dass die USA „Wirtschaftsterrorismus“ betrieben hätten, um unschuldige iranische Bürger zu töten und ihnen den Zugang zu dringend benötigter medizinischer Versorgung zu verwehren.⁶⁷ Zarifs Rede nahm die Anordnung des Obersten Führers nicht zur Kenntnis, die ein staatliches Importverbot für westliche Impfstoffe beinhaltete.⁶⁸ Solche Beispiele zeigen, dass Regierungsvertreter versucht haben, den globalen Diskurs über den Iran zu manipulieren, um die wirtschaftliche Not des Landes von den Auswirkungen der entschlossenen Prioritätensetzung der Regierung abzukoppeln.

Ein weiteres Beispiel für die Bemühungen der Regierung, den globalen Diskurs über den Iran zu manipulieren, ist der Diskurs über den internen Kampf zwischen den „Pragmatikern“ und den „Hardlinern.“ Der frühere Präsident Rohani und sein außenpolitisches Team, angeführt vom ehemaligen Außenminister Zarif, haben sich wiederholt als prowestliche und friedliche Fraktion der politischen Elite dargestellt, die in allen Aspekten der Politikgestaltung gegen das gegnerische Lager der Hardliner kämpfen musste, insbesondere in Bezug auf das Atomabkommen. Kurz nach dem Ende seiner Amtszeit als Außenminister des Landes wurde ein aufgezeichnetes Interview mit Zarif im Internet verbreitet, in dem er behauptete, dass die Revolutionsgarden die Entscheidungen des Außenministeriums überstimmt und untergraben hätten. Er behauptete, dass die diplomatischen Bemühungen seines Teams zur Lösung der Krise um das Atomprogramm des Landes durch die Pläne der Revolutionsgarden in den regionalen Kriegen unterminiert worden seien. Diese seien von der strategischen Vision des verstorbenen Generals Soleimani angeführt worden. Die Revolutionsgarde, die vom Obersten Führer des Landes geleitet wird, verfolge eine strategische Vision, die mit der des Obersten Führers übereinstimme. Die Be-

hauptungen von Zarif und Rohani wurden weithin (inner- und außerhalb des Landes) als Zeichen für ein Gleichgewicht des Machtkampfes um die strategische Ausrichtung des Irans zwischen dem Obersten Führer, dem Präsidenten und seinem Außenminister wahrgenommen. Eine kürzlich durchgeführte Studie deutet darauf hin, dass keine Konkurrenz (wie von Zarif behauptet), sondern eine enge Koordination der außenpolitischen Entscheidungsfindung der iranischen Regierung zwischen diesen drei hochrangigen Persönlichkeiten existierte.⁶⁹

Es gibt noch einen weiteren Aspekt der Diskursmanipulation im iranischen Informationskrieg. Im Jahr 2023 tauchten eine Reihe von gehackten E-Mails und Online-Kommunikationsaufzeichnungen zwischen mehreren Experten und Analysten iranischer Herkunft auf, die in prominenten Thinktanks und an westlichen Universitäten gearbeitet haben. Diese Personen und ihre Analysen haben den globalen, insbesondere den westlichen Diskurs über den Iran maßgeblich geprägt. Ihre Analysen zum Iran haben die Medien und viele Politikanalysen praktisch dominiert, insbesondere in den Jahren vor dem Abschluss des Atomabkommens. Die durchgesickerten Dokumente zeigten die Intensität und den Umfang der Zusammenarbeit zwischen dieser Gruppe von Iran-Experten und dem iranischen Außenministerium.⁷⁰ Offenkundig hat die iranische Regierung ein Netzwerk von Experten und Analysten gebildet, das weltweit als „Irans Experteninitiative“ bekannt wurde.⁷¹ In Medienberichten wurde auf unterschiedliche Formen der Koordination zwischen diesem Netzwerk und der iranischen Regierung hingewiesen. Dabei wurde auch der Vorwurf geäußert, dass sich in westlichen Thinktanks arbeitende Iran- oder Nahost-Experten ihre Artikel von iranischen Regierungsstellen hätten vorformulieren lassen. Auch hätten einzelne Experten eine Art von Verpflichtungserklärung gegenüber dem iranischen Außenministerium abgegeben. Dabei sei es um die Zustimmung des Außenministeriums für Analysen gegangen, die über den Iran oder die Lage im Nahen Osten veröffentlicht werden sollten.⁷² Mehrere der dort genannten Experten haben sich zu den durchgesickerten Dokumenten geäußert und die Authentizität der gehackten Dokumente bestätigt. Sie argumentierten aber, dass ihre Zusammenarbeit mit den iranischen Beamten nicht außergewöhnlich gewesen sei

⁶⁶ How have sanctions affected Iran? Imam Khamenei explains, *Webseite Khamenei.ir*, 8.1.2019.

⁶⁷ T Medicine import impossible due to sanctions, Iranian health minister writes to WHO chief, *Tehran Times online*, 1.1.2020.

⁶⁸ Golnaz Esfandiari: Khamenei's Ban On Western Vaccines Blasted As A 'Politicization' Of Iranians' Well-Being, *Radio Free Europe/Radio Liberty online*, 12.1.2021.

⁶⁹ Bazoobandi/Heibach/Richter 2023.

⁷⁰ Boyorgmehr Sharafian: Inside Tehran's Soft War, *Iran International* (2023), <https://content.iranintl.com/en/investigates/inside-tehran-softwar/index.html>.

⁷¹ Graeme Wood: Iran's Influence Operation Pays Off, *The Atlantic online*, 28.9.2023.

⁷² Jay Solomon: How Iran used its ties to a top global NGO, *www.Semafor.com*, 24.2.2024.

und tatsächlich Teil ihrer täglichen beruflichen Aufgaben wäre. Ob die in den geleakten Dokumenten genannten Experten (meist Abkömmlinge von Exiliranern) tatsächlich von der iranischen Regierung kooptiert wurden, ist von außen schwer zu beurteilen. Der Einfluss ihrer Arbeit auf die Führung des politischen Diskurses zur iranischen Regierung kann jedoch nicht geleugnet werden.

Warum haben sich möglicherweise iranisch-stämmige Experten in westlichen Ländern zur Kooperation mit iranischen Regierungsstellen verleiten lassen? Es gibt zwar nicht viele öffentlich zugängliche Informationen über die dabei angebotenen Anreize, aber in den meisten Fällen wurde diesen Personen ein privilegierter Zugang zum inneren Kreis der iranischen Entscheidungsträger und das Recht auf sichere Reisen in ihr Heimatland gewährt. Beides ist für unabhängige und vertrauenswürdige Analysten und Wissenschaftler praktisch unmöglich. Es gibt eine hohe Zahl an iranischen Akademikern, Forschern und Journalisten mit doppelter Staatsbürgerschaft, die im Laufe der Jahre in den iranischen Gefängnissen festgehalten wurden.

8 Schlussfolgerung

Die Strategien und Methoden des Irans in seiner Informationskriegführung haben sich im Laufe der Zeit verändert und sind einen Entwicklungsprozess durchlaufen. Die Regierung in Teheran hat sowohl im In- als auch im Ausland massiv in mehr oder weniger ausgeklügelte Methoden und Instrumente zur Durchführung von Informationskriegführung investiert. Die politische Ideologie der Regierung hat bei der Wahl der Strategien und Methoden eine bedeutende Rolle gespielt. Das ideologische Konzept des „Sieges durch Angst“ war und ist die Grundlage für die Institutionalisierung der Angst in der iranischen Informationskriegführung. Die Regierung hat in ihrem Informationskrieg gegen politische Dissidenten inner- und außerhalb des Landes institutionell menschliche Emotionen als Strategie der Abschreckung eingesetzt. Sie hat auch massiv in ausgeklügelte cybergestützte Beeinflussungsoperationen investiert, die von iranischen Organisationen oder über Cyber-Stellvertreter durchgeführt werden. Darüber hinaus hat die Regierung ein globales Netzwerk von Agenten und Sympathisanten durch religiöse, kulturelle und akademische Institutionen aufgebaut. Vieles deutet darauf hin, dass die Revolutionsgarden ein wichtiger Akteur in der iranischen Informationskriegführung waren. Die mächtigste politische Figur in der iranischen Regierung, der Oberste Führer des Landes, ist der Oberbefehlshaber der Streitkräfte, zu denen auch die Revolutionsgarden gehören.

Nach der politischen Ideologie der iranischen Regierung besitzt der Führer auch ein hohes Maß an göttlicher Macht. Vor diesem Hintergrund zeigt ein Blick auf die Informationskriegführung des Landes, dass der Oberste Führer eng an der Ausarbeitung und Umsetzung der Strategien beteiligt war. Dies spiegelt sich insbesondere in seinen engen Beziehungen zu den vom Iran gesponserten islamischen Zentren auf der ganzen Welt wider, unter anderem in Großbritannien und Deutschland. Schließlich deutet die Untersuchung der Diskursmanipulationstaktiken der Regierung darauf hin, dass die Bemühungen, den globalen Diskurs gegenüber dem Iran zu manipulieren, auf verschiedenen Ebenen inner- und außerhalb des Landes unternommen werden. Die Regierung hat die Beziehungen zu gleichgesinnten Ländern wie China und Russland vorangetrieben, die Teherans geopolitische Vision für eine Welt teilen. Letztere ist darauf ausgerichtet, die westlichen Mächte, insbesondere die USA und ihre Verbündeten, zu schwächen und gleichzeitig ihre eigene Macht zu projizieren. Daher ist zu erwarten, dass die Koordinierung, der Informationsaustausch und die technologische Zusammenarbeit zwischen dem Iran und diesen Ländern zunehmen werden. Dies wird die Fähigkeiten der iranischen Regierung erhöhen und ihre Strategien zur Durchführung von Informationskriegführung weiter vorantreiben.

Literatur

- Amiri, Abulfazl/Nafavi, Hamid (2016): Psychological Operation and its Impact on Urban Uprisings [شهری اغتشاشات بر آن تأثیر و روانی عملیات], *Quarterly Journal of Crisis Management and Emergencies*, 7 (27), 51–82
- Anderson, Collin/Sadjadpour, Karim (2018): *Iran's cyber threat, espionage, sabotage, and revenge*. Washington, D. C.: Carnegie Endowment for International Peace
- Banikamal, A./Ra'ees, W. (2018): Iran's Educational Diplomacy in the Muslim World. *Insight Turkey*, 20 (1), 165–188
- Bazoobandi, Sara (2023): Populism, jihad, and economic resistance: Studying the political discourse of Iran's supreme leader, *Digest of the Middle East Studies*, 32 (4), 1–19
- Bazoobandi, Sara/Heibach, Jens/Richter, Thomas (2024): Iran's foreign policy making: consensus building or power struggle? *British Journal of Middle Eastern Studies*, 51 (im Erscheinen)
- Cohen, Ronen A. (2022): Reframing al-Quds Day as a unifying Islamic symbol: the battle over Jerusalem between Iran and the Arab world, *Contemporary Islam*, 16, 335–352
- Council on Foreign Relations (2021): *The Iran-Russia Cyber Agreement and U. S. Strategy in the Middle East*. Washington, D. C.: CFR
- Freilich, Chuck (2024): *The Iranian Cyber Threat*. Tel Aviv: The Institute for National Security Studies
- Microsoft Threat Intelligence (2024): *Iran surges cyber-enabled influence operations in support of Hamas. A Report*. Redmond, Wash.: www.microsoft.com/en-us/security/business/security-insider/reports/

iran-surges-cyber-enabled-influence-operations-in-support-of-hamas/

Office of the Director of National Intelligence (2023): *Annual Threat Assessment of the United States (US) Intelligence Community*. Washington, D. C.: Director of National Intelligence

Theohary, Catherine A. (2020): *Iranian Offensive Cyberattack Capabilities*. Washington, D. C.: Congressional Research Service

United States Air Force (2023): *Air Force Doctrine Publication 3–13, Information in Air Force Operations*. Washington, D. C.: US Department of Defense

United States Department of Defense (2012): *Information Operations*. Washington, D. C.: US Department of Defense

United States Navy (2020): *Naval Doctrine Publication, Naval Warfare*. Washington, D. C.: US Department of Defense

Zusatzmaterial: Die Onlineversion bietet als Zusatzmaterial eine englische Übersetzung des Artikels (<https://doi.org/10.1515/sirius-2024-4002>).