Nr. 531/ August 2024
Analysen & Argumente

KONRAD ADENAUER STIFTUNG

Cyber-Actors: Iran

Wie Angriffe auf den Staat stark machen

Ferdinand A. Gehringer, Julia Kramer

- Der Stuxnet-Angriff und die digitale Organisation von Massendemonstrationen waren Schlüsselereignisse, durch die sich der Iran zu einem ernst zu nehmenden Akteur im Cyber- und Informationsraum entwickelte.
- Heute verfügt der Iran über höchst professionelle Cybereinheiten, um das breite Operationsspektrum im digitalen Raum abzudecken.
- Die offensiven Cyberoperationen zielen auf Spionage, Sabotage und Einflussnahme ab – iranische APT-Gruppen sind in der Lage, ihren operativen Schwerpunkt schnell und flexibel den aktuellen geopolitischen Anforderungen anzupassen.
- Der Iran agiert in Deutschland unter anderem mit APT 42 (auch Charming Kitten genannt) und hat politische und Menschenrechtsaktivistinnen und -aktivisten, Medienschaffende sowie Frauenrechtlerinnen und Frauenrechtler als Operationsziele.
- Jedoch sind auch die iranischen Cyberkapazitäten begrenzt – zum einen fehlt es in der Breite an gut ausgebildetem Personal, um den ständigen Angriffen begegnen zu können, zum anderen ist das Land immer noch sehr abhängig von westlichen Soft- und Hardware-Technologien.
- Deutschland ist als enger Verbündeter der USA und Israels ebenso stark im Fokus des Regimes und muss sich neben Spionageaktivitäten auch auf Sabotageakte einstellen und Gegenmaßnahmen ergreifen.

Inhaltsverzeichnis

Seit den Jahren 2009 und 2010 baut der Iran energisch seine digitalen Kapazitäten aus. Das Land hat erhebliche Sicherungs- und Schutzmaßnahmen ergriffen, seine Fähigkeiten im Cyber- und Informationsraum fortentwickelt und verfügt heute über eine wirkungsstarke „Cyberarmee".

Äußere Einwirkungen fördern digitales Aufrüsten

In der ersten Entwicklungsphase reagiert der Iran mit Schutzmechanismen und baut seine Cyberorganisationsstruktur um.

2009 nutzte die iranische Opposition sehr effektiv das Internet, um nach den manipulierten Präsidentschaftswahlen Massendemonstrationen zu schüren. Die Proteste konnte das Regime noch unterdrücken, doch hinterließen die Einflussmöglichkeiten auf die Gesellschaft durch das Internet einen bleibenden Eindruck.[1] Im Jahr 2010 führte der Stuxnet-Angriff[2] dazu, dass die Leittechnik (Zentrifugen) der Urananreicherungsanlage in Natanz und des Kernkraftwerks Buschehr abgeschaltet werden mussten. Circa 20 Prozent der gesamten Zentrifugen in Natanz wurden zerstört.[3] Es war der weltweit erste bekannt gewordene Cyberangriff, der einen unmittelbaren physischen Schaden erzeugte.

Als Reaktion auf den Stuxnet-Angriff und die Entwicklung des Computerwurmes Flame[4] erhöhte das Regime den digitalen Schutz seines Atomprogramms. Weitere Vorfälle und Angriffe führten in der Folgezeit zu einem sukzessiven Aufrüsten. Ein Cyberangriff im Juli 2021 auf die Systeme der nationalen Eisenbahngesellschaft mit der Wiper-Schadsoftware[5] MeteorExpress brachte den Zugverkehr zum Erliegen. Die Webseiten der staatlichen Eisenbahnbehörde mussten vom Netz genommen werden, Anzeigetafeln wurden manipuliert und der Zugverkehr nach Fahrplanstörungen unterbrochen.[6] In einem Stahlwerk im Süden des Landes musste die Produktion gestoppt werden, nachdem ein Cyberangriff im Juni 2022 die Systeme des Werkes störte. Ein mutmaßlicher Cyberangriff im Dezember 2023 auf die Bezahlsoftwaresysteme von Tankstellen, für den der Iran Israel verantwortlich machte, führten zu einem landesweiten Ausfall der Kraftstoffversorgung. Teheran veranlasste im Zuge dessen, dass die Schlüsselsektoren des Landes besonders geschützt werden. Die Absicherungsmaßnahmen der Industrial Control Systems (ICS)[7] wurden verschärft und das Schwachstellenmanagement in kritischen Einrichtungen verbessert.[8] Auch der Informationsraum wird genutzt, um einzuwirken. Kritiker des Regimes und Oppositionelle bedienen sich sozialer Medien, um ihre Meinungen kundzutun.[9] Vor zwei Jahren wurden Systeme des Betreibers des iranischen Staatsfernsehens kurzzeitig übernommen und über die Sender regimefeindliche Inhalte gesendet.[10]

Verschiedene Organisationen bilden schlagfertige Cybereinheiten

Umfassende Strukturreformen stärken den staatlichen Cyberapparat.

Auf Anweisung des Obersten Führers des Iran wurde im März 2012 eine neue Organisationsstruktur geschaffen. Der Oberste Cyber-Rat (SCC) wurde eingerichtet und mit der Planung und Umsetzung einer Cyberspace-Strategie[11] sowie von Richtlinien[12] beauftragt. Damit war der Iran einer der ersten Staaten weltweit mit einer Strategie. Der SCC setzt sich aus hochrangigen Regierungsvertretern wie dem Präsidenten des Iran, dem Leiter der Justiz und des Parlaments, dem Leiter des staatlichen Rundfunks und der Polizei sowie aus den Ministern für Geheimdienst, Telekommunikation, Kultur, Wissenschaft und dem Oberbefehlshaber der Islamischen Revolutionsgarde zusammen. Die Islamische Revolutionsgarde (IRGC)[13] ist das wichtigste Mitglied des SCC. Deren hochqualifizierte Einheiten für elektronische Kampfführung und Cyberverteidigung tragen die Hauptverantwortung für offensive Cyberoperationen. Die IRGC unterstützt zudem Operationen iranischer Proxys wie zum Beispiel der Hisbollah. Diese sind ebenfalls Teil der Cyberarmee und werden als *Advanced-Persistent-Threat* Gruppen (APT)[14] eingestuft.

Die IRGC kontrolliert auch die Basij Miliz. Diese umfasst circa 1.000 Cybereinheiten. Außerdem hat sie Zugriff auf circa 50 verschiedene Hackergruppen.[15] Die Basij verfügt über eine Troll-Armee, die in sozialen Medien, Blogs und Foren regimekritische Äußerungen löscht und eigene Propaganda verbreitet.[16] Die Befehlsstrukturen zwischen IRGC, Basij und auch den Hackergruppierungen sind fließend und Teil einer Verschleierungstaktik. Aktivitäten lassen sich hierdurch schwer vorhersehen und einem bestimmten Akteur zuordnen (Attribution). Pro-iranische Hackergruppen und deren Cyberaktivitäten werden staatlich gebilligt.[17] Sofern sie keine staatlichen Interessen beeinträchtigen, werden ihre (kriminellen) Operationen nicht verfolgt und Rechtshilfeersuchen anderer Staaten abgeblockt.

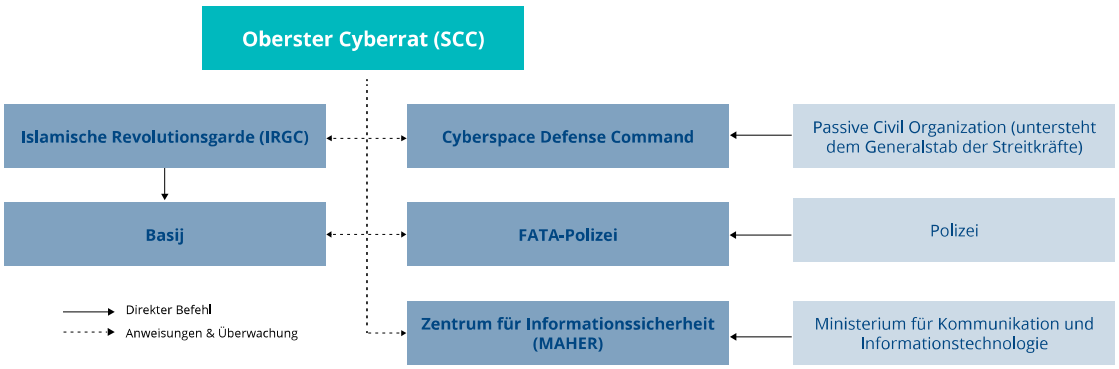
Die zweiten Entwicklungsphase ist geprägt vom Ausbau defensiver Cyberfähigkeiten und dem Aufbau von Technologie-Partnerschaften mit Moskau und Peking.

Eine weitere zentrale Organisation ist das *Cyberspace Defense Command*, das unter Aufsicht der Passiven Zivilverteidigung steht, die wiederum zum Generalstab der Streitkräfte gehört. Das *Cyberspace Defense Command* ist mit defensiven Aufgaben betraut und entwickelt eine umfassende Verteidigungsdoktrin für staatliche Institutionen und Infrastrukturen gegen Cyberbedrohungen.[18]

Das Komitee zur Identifizierung nicht genehmigter Standorte und die FATA-Polizei[19] bilden die Cyberpolizei. Sie überwachen die Internetnutzung und bekämpfen Internetkriminalität.[20] Die Spezialisten infiltrieren Webseiten und E-Mail-Konten, identifizieren Betreiber und leiten Strafverfolgungen ein. Die FATA-Polizei übt zudem Druck auf Internetdienstanbieter oder Besitzer von Internetcafés aus, damit diese ihnen Daten und Auskünfte über Internetnutzer bereitstellen.[21] Sie arbeitet eng mit den Justizbehörden zusammen und berichtet an den Hohen Rat.[22]

Für die Cybervorfallsbekämpfung wurde das Zentrum für Informationssicherheit (MAHER) eingerichtet. Es entwickelt Reaktionsmechanismen für Krisenfälle, verfügt über Incident Response Teams[23] und betreibt Wissensmanagement. Das Zentrum bildet Fachkräfte aus und ist zuständig für den Schutz der staatlichen Webseiten sowie einiger privater Unternehmen.[24]

Organisation der Cybereinheiten



Quelle: eigene Darstellung

Das Budget für den Ausbau der Fähigkeiten im Cyber- und Informationsraum ist zwischen 2013 und 2021 um das Zwölffache gestiegen.[25] Berichten zufolge betrugen bis 2016 die jährlichen Ausgaben circa eine Milliarde US-Dollar. Im Vergleich dazu gab das Vereinigte Königreich, eine der am weitest entwickelten Staaten im Hinblick auf die Fähigkeiten im Cyber- und Informationsraum, um die zwei Milliarden US-Dollar aus.

Spezialisiertes und arbeitsteiliges Operieren entwickeln sich fort

Staatliche Hackergruppen nehmen auch immer mehr westliche Nationen in den Blick.

Die offensiven Cyberoperationen zielen neben Sabotage und Spionage auch auf Einflussnahme ab. Staatlich instruierte Hacker zeigten 2012 zum ersten Mal ein koordiniertes Vorgehen und verbesserte Fähigkeiten. Die eigens entwickelte Schadsoftware Shamoon zerstörte die IT-Infrastruktur von Saudi-Aramco, dem staatlichen Energieunternehmen Saudi-Arabiens. Mehrere zehntausend Computer wurden damals unbrauchbar gemacht. Eine proiranische Gruppe griff US-Banken mit einer massiven DDoS-Attacke[26] an. Kunden hatten temporär keinen Online-Zugriff auf ihre Bankkonten. Zeitgleich versuchte eine andere Einheit, die Kontrolle über einen Staudamm nahe New York City zu übernehmen.[27] Im Herbst 2019 veröffentlichte Microsoft einen Bericht, der darlegte, dass sich eine hochprofessionell agierende iranische APT-Gruppe verstärkt um Zugang zu Unternehmen bemüht, die Industrial Control Systems (ICS) herstellen, verkaufen oder warten. Wer ICS kontrolliert, kann Kraftwerke, Stromnetze und Produktionsanlagen manipulieren.[28] Im April 2020 wurde ein Cyberangriff vereitelt, der die Wasserversorgung Israels stören sollte.[29] Seit mindestens 2014 fokussiert sich Magic Hound (auch APT 35) auf Spionageoperationen gegen Regierungs- und Militärangehörige in Europa, den USA und dem Nahen Osten sowie gegen Akademikerinnen und Akademiker, Journalistinnen und Journalisten sowie internationale Organisationen (wie die WHO).[30] In Deutschland ist der Iran über Charming Kitten (auch APT 42) aktiv. Laut dem Bundesamt für Verfassungsschutz hat Charming Kitten politische und Menschenrechtsaktivistinnen und -aktivisten und iranische Oppositionelle[31], Medienschaffende und Frauenrechtlerinnen und Frauenrechtler im Visier.

In der dritten Entwicklungsphase folgt der Ausbau der offensiven Cyberfähigkeiten.

Iranische Cyberakteure passen ihre Ziele den gegenwärtigen Interessen des Regimes an. Zu Beginn der Corona-Pandemie führten Hackergruppen Operationen gegen den Pharmasektor aus. Die Hackergruppe Polonium hat sich auf den Konflikt mit Israel im Cyberraum spezialisiert und setzt gezielt Malware gegen Ingenieur-, IT-, Rechts-, Kommunikations-, Marketing- und Versicherungsunternehmen in Israel ein.[32] Wiederum andere sind für die Verfolgung in- und ausländischer Oppositionsgruppen (vor allem vor den iranischen Präsidentschaftswahlen) verantwortlich.[33]

Eigene Cloud-Struktur soll zu mehr gesellschaftlicher Kontrolle führen

Mit eigenen Forschungs- und Entwicklungsprogrammen und Kooperationen mit Russland und China soll Abhängigkeit verringert werden.

Die iranischen Cyberkapazitäten sind allerdings begrenzt. Zum einen fehlt es in der Breite an gut ausgebildetem Personal, um ständigen Angriffen beispielsweise Israels und der USA begegnen zu können, und zum anderen ist die Islamische Republik abhängig von westlichen Soft- und Hardware-Technologien.[34] Seit 2015 schlossen Russland und der Iran immer wieder Abkommen über gemeinsame Kooperationen, die vom Aufbau gemeinsamer Cyberfähigkeiten, der Bereitstellung von russischer Überwachungssoftware über die Zusammenarbeit bei der Entwicklung von alternativen Softwarelösungen zu US-Produkten, der Förderung der Zusammenarbeit bei 5G-Netzen und KI, die diplomatische Koordination in der UN und anderen multilateralen Foren, um internationale Cybernormen und -gesetze zu fördern, bis hin zur Verständigung auf die gegenseitige Förderung von Medieninhalten und Koproduktionen, um westlichen Narrativen entgegenzuwirken, reichen. 2021 folgte das bisher umfassendste bilaterale Paket für die Informationssicherheit. Es ist davon auszugehen, dass der Iran Technologien an die Hisbollah weitergibt. 2021 schlossen China und der Iran ein Abkommen über eine strategische Zusammenarbeit. Dieses umfasst unter anderem die chinesische Unterstützung beim Aufbau der iranischen 5G-Telekommunikationsinfrastruktur, den Zugang zum chinesischen Satellitennavigationssystem Beidou und die Unterstützung bei der Stärkung des staatlichen Machtapparates. Zudem könnte es auch die Förderung der iranischen Cyberfähigkeiten umfassen.[35]

Ein 2009 entwickeltes Nationales Informationsnetzwerk (NIW) versetzt den Iran in die Lage, effektiver ausländische und inländische kulturelle und politische Einflüsse zu bekämpfen, Quellen zu überwachen, zu identifizieren und seine Anfälligkeit für externe Cyberangriffe zu verringern. Inländische Unternehmen verlagerten ihre Netzwerkaktivitäten auf Server und Datenzentren im Iran, um hiesige Webseiten selbst hosten und kontrollieren zu können.[36] Einigen Berichten zufolge verfügt das Regime auch über einen unabhängigen E-Mail-Dienst und ein Betriebssystem.

Das nationale Intranet wurde nach chinesischem Vorbild aufgebaut.

Der größte iranische Cloud-Service-Anbieter Arvancloud entwickelt derzeit eine nationale Cloud-Struktur, die Iran Cloud. Hierdurch wird das Regime in der Lage sein, bestimmte Bereiche kontrolliert vom globalen Internet abzuschotten und Teilnetze abzuschalten. Mittel- bis langfristig sollen möglichst viele Unternehmen in diese nationale Cloud-Struktur eingebunden werden. Während Wirtschaftsunternehmen weiterhin am globalen Internetverkehr teilnehmen, kann die Zivilgesellschaft abgeschottet werden. Nach dem Tod von Mahsa Amini 2022 hat das Regime einzelne Webseiten und Dienste wie WhatsApp, Instagram, Telegram, Signal sperren lassen und die Datenübertragung gedrosselt, sodass Demonstrierende Schwierigkeiten hatten, sich digital zu koordinieren.[37]

Es wird ferner vermutet, dass über das Unternehmen Softqloud ein Tochterunternehmen in Deutschland betrieben wird. Die Softqloud-Server in Düsseldorf sind für die Iran Cloud von entscheidender Bedeutung, da sie eine der wenigen digitalen Verbindungsbrücken bilden, eine dezentrale Vernetzung von Servern ermöglichen und etwaige Ausfälle der Iran Cloud kompensieren können.[38]

Vorgehen des Regimes gegen Israel und USA sollte Deutschland warnen

Der Iran baut seine offensiven Fähigkeiten weiter aus und nimmt weltweit vermehrt den IT- und Technologiesektor, die Rüstungsindustrie und Kritische Infrastrukturen in den Fokus seiner offensiven Operationen. Zugleich passt er seine Ziele entsprechend geopolitischer Entwicklungen (Corona-Pandemie, russischer Angriffskrieg auf die Ukraine, Terrorismusbekämpfung in Gaza) an. Derzeit werden die Fähigkeiten und Aktivitäten des Regimes noch unterschätzt. Deutschland als enger Verbündeter der USA und Israels ist stark im Fokus. Die diplomatischen Räume des Regimes in der Bundesrepublik Deutschland sind deutlich eingeschränkt und Informationskanäle sind begrenzt. Das führt zu einer Verlagerung der Spionageaktivitäten von Human Intelligence zur Fernmeldeaufklärung in den Cyber- und Informationsraum. Auch Sabotageakte an Kritischen Infrastrukturen werden wahrscheinlicher. Sicherheitsbehörden und Verfassungsschutz müssen im Rahmen der Spionageabwehr vermehrt iranische Akteure im Visier haben, Kritische Infrastrukturen ihr Schutzniveau erhöhen und neben Sicherheits- auch Resilienzmaßnahmen ergreifen. Die Bundesrepublik Deutschland sollte dringend Wissenschaftskooperationen begrenzen und Technologiepartnerschaften mit dem Regime unterbinden (vor allem im Bereich Kritischer Infrastrukturen und IT-Dienstleistung). Zudem sollte die Tätigkeit von Softqloud in Deutschland über Ermittlung des Staatsschutzes oder Untersuchungen wegen Sanktionsverstößen nun endlich überprüft werden. Auf internationaler Ebene sollte Deutschland weiterhin für die Freiheit des Internets einstehen und eine Fragmentierung verhindern. Die Strategie für die Internationale Digitalpolitik der Bundesregierung enthält keine wirkmächtigen Instrumente für die Durchsetzung der Freiheit des Internets. Ein Hebel wäre die große Abhängigkeit des iranischen Regimes von deutschen Exporten (chemische oder pharmazeutische Erzeugnisse).

Ein sich zuspitzender Konflikt mit dem Iran kann auch im Cyber- und Informationsraum für Deutschland erhebliche Folgen haben.

1 Kausch, Kristina und Tabansky, Lior (2018): Cybered Conflict in the Middle East, Mediterranean Dialogue Series No. 15 (Konrad-Adenauer-Stiftung): S. 9; Anderson, Collin und Sadjadpour, Karim (2018). Iran's Cyber Threat: Espionage, Sabotage and Revenge (Carnegie Endowment for International Peace): S. 10 f.

2 Ein von den USA und vermutlich auch von Israel initiierter Cyberangriff auf das Atomprogramm der Islamischen Republik Iran. Der Angriff trägt den Namen der Schadsoftware Stuxnet.

3 Akhtar, Noureen (2023): Emerging Cyber Security Challenges: Implications for Iranian National Security, BTTN Journal 2(2): S. 92.

4 Flame wurde vermutlich von den USA und Israel entwickelt. Er war ein hochkomplexer und fortschrittlicher Computerwurm, der 2012 entdeckt wurde und dazu diente, gezielt sensible Informationen aus Regierungseinrichtungen, Unternehmen und von Privatpersonen zu stehlen.

5 Wiper-Malware ist eine Art von Schadprogramm, das darauf abzielt, Daten von einem infizierten System zu löschen oder zu beschädigen, anstatt sie zu stehlen oder zu manipulieren.

6 Mäder, Lukas (2021): Kein Benzin an den Tankstellen und Probleme im Zugverkehr, Neue Züricher Zeitung.

7 Industrial Control Systems (ICS) sind ein wesentlicher Bestandteil der industriellen Infrastruktur. Zu diesen Systemen gehören u. a. verteilte Steuerungssysteme (Distributed Control Systems, DCS) und auch Überwachungs- und Datenerfassungssysteme (Supervisory Control and Data Acquisition Systems, SCADA).

8 Akhtar, Noureen (2023): Emerging Cyber Security Challenges: Implications for Iranian National Security, BTTN Journal 2(2).

9 Ebd., S. 96.

10 Vgl. https://www.tagesschau.de/faktenfinder/kontext/iran-desinformation-101.html (letzter Abruf: 28.06.2024).

11 Siboni, Gabi und Kronenfeld, Sami (2012): Iran and Cyberspace Warfare, INSS Military and Strategic Affairs 4(3): S. 87 ff.

12 Vgl. http://www.strato-analyse.org/fr/spip.php?article223#nh1 (letzter Abruf: 28.06.2024).

13 Bei der IRGC handelt es sich um einen Staat im Staate: Sie wurde 1979 gegründet, da die neuen Machthaber dem vom Schah aufgebauten Militär misstrauten. Daher unterhält die Revolutionsgarde beispielsweise einen eigenen Nachrichtendienst, der unabhängig vom offiziellen Nachrichten-dienst der Regierung agiert und direkt an das Büro des Revolutionsführers berichtet. Zusammen mit der regulären Armee bildet die IRGC heute die Streitkräfte des Iran und untersteht Ayatollah Khamenei. Originär hat sie den Auftrag, die innerstaatliche Sicherheit zu schützen, Putsche zu verhindern und die Staatsideologie zu bewahren und zu verbreiten.

14 Originär bezeichnet Advanced Persistent Threat (APT) einen vielschichtigen, zielgerichteten und effizienten Angriff auf IT-Infrastrukturen und Daten. Einige dieser Angriffe werden je nach vermuteter Herkunft des Angreifers oder nach dem Vorgehen zur späteren Wiedererkennung mit einer Nummerierung versehen.

15 Dazu gehören die Iranische Cyberarmee, Islamische Cyberwiderstandsgruppe und das Ashiyane Team für digitale Sicherheit und verschiedene Untergruppen der Kitten-Gruppe. Flying Kittens sammeln Informationen über ausländische Regierungen und Unternehmen von Interesse; Magic Kittens zielen auf inländische Dissidenten; Domestic Kittens zielen auf Dissidenten im Iran, den Vereinigten Staaten, dem Vereinigten Königreich und anderen Ländern; Charming Kittens nutzen soziale Netzwerkplattformen, um verschiedene Ziele zu erreichen und Cutting Kittens produzie-ren Tools zum Eindringen in Webseiten.

16 Vgl. http://www.strato-analyse.org/fr/spip.php?article223 (letzter Abruf: 28.06.2024).

17 Denning, Dorothy (2020): Explainer: How Iran's Military Outsources its Cyberwarfare Forces, Navy Times.

18 Akhtar, Noureen (2023): Emerging Cyber Security Challenges: Implications for Iranian National Security, BTTN Journal 2(2): S. 95 ff.

19 Die FATA-Polizei ist eine Einheit der Polizei der Islamischen Republik. FATA ist die persische Abkürzung für „Die Polizei für den Bereich der Pro-duktion und des Austauschs von Informationen".

20 Brunner, Jordan A. (2017): The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergency, Jurimetrics Journal 57(3): S. 397–431.

21 Vgl. http://www.strato-analyse.org/fr/spip.php?article223 (letzter Abruf: 28.06.2024).

22 Akhtar, Noureen (2023): Emerging Cyber Security Challenges: Implications for Iranian National Security, BTTN Journal 2(2): S. 97.

23 Incident Response Teams (IRTs) im Bereich von Cyberangriffen sind Gruppen von Experten, die darauf spezialisiert sind, auf Sicherheitsvorfälle im Zusammenhang mit Informationstechnologie und Computersystemen zu reagieren. Ihre Aufgaben umfassen die Erkennung, Analyse, Eingren-zung und Behebung von Sicherheitsvorfällen, um die Auswirkungen zu minimieren und die Integrität, Vertraulichkeit und Verfügbarkeit der betroffenen Systeme und Daten zu schützen.

24 Dr. Siboni, Gabi und Kronenfeld, Sami (2012): Iran and Cyberspace Warfare, INSS Military and Strategic Affairs 4(3): S. 84.

25 Siboni, Gabi, Abramski, Léa und Sapir, Gal (2020): Iran's Activity in Cyberspace, Cyber, Intelligence, and Security 4(1): S. 22; International Institute for Strategic Studies (2021): Cyber Capabilities and National Power; Pahlavi, Pierre: Digital Hezbollah and Political Warfare in Cyberspace, Nation-al Interest, 31. Oktober 2022.

26 DDoS steht für Distributed Denial of Service. Hierbei handelt es sich um eine Form des Cyberangriffs, bei der innerhalb kurzer Zeit sehr viele Anfragen auf einen Server, eine Webseite oder eine Netzwerkressource erfolgen, die zur Überlastung führen. Hierdurch wird die Anwendung außer Betrieb gesetzt.

27 Muth, Max (2019): Kalter Krieg im Netz, Süddeutsche Zeitung.

28 Brühl, Jannis (2020): Auch im Netz haben sie eine Rechnung offen, Der Bund.

29 Vgl. https://www.sueddeutsche.de/politik/israel-angriff-auf-wasserversorgung-1.4921359 (letzter Abruf: 28.06.2024).

30 Vgl. https://attack.mitre.org/groups/G0059/ (letzter Abruf: 28.06.2024).

31 Vgl. ClearSky Cyber Security (2017): Charming Kitten: S. 3.

32 Vgl. https://www.pressetext.com/news/20221116010 (letzter Abruf: 28.06.2024).

33 Vgl. https://www.mandiant.com/resources/blog/apt42-charms-cons-compromises (letzter Abruf: 28.06.2024).

34 Akhtar, Noureen (2023): Emerging Cyber Security Challenges: Implications for Iranian National Security, BTTN Journal 2(2): S. 102.

35 Fassihi, Farnaz und Myers, Steven Lee: Defying U.S., China and Iran Near Trade and Military Partnership, New York Times, 11. Juli 2020; Fassihi, Farnaz und Myers, Steven Lee: China, With $400 Billion Iran Deal, Could Deepen Influence in Mideast, New York Times, 27. März 2021; Pinko, Eyal: Iranians Developing the Cyber Capabilities of Hezbollah, Israel Defense, 30. März 2021; Esfandiari, Golnaz: Iran to Work With China to Create National Internet System, Radio Free Europe, Radio Liberty, 4. September 2020.

36 Alimardani, Mahsa (2016): Iran Declares 'Unveiling' of its National Intranet, Advox.

37 Baeck, Jean-Philipp (2022): Die Iran Connection von Meerbusch, TAZ.

38 Drucksache 20/4515 (2022): Antwort der Parlamentarischen Staatssekretärin Rita Schwarzelühr-Sutter vom 18. November 2022 auf schriftliche Frage von J. Hardt MdB, https://dserver.bundestag.de/btd/20/045/2004515.pdf (letzter Abruf: 28.06.2024).

Impressum

Die Autorin und der Autor

Julia Kramer ist Wissenschaftliche Mitarbeiterin in der Abteilung Internationale Politik und Sicherheit.

Ferdinand A. Gehringer arbeitet als Policy Advisor für Innere und Cybersicherheit in der Abteilung Internationale Politik und Sicherheit.

Konrad-Adenauer-Stiftung e. V.

Ferdinand Gehringer
Abteilung Internationale Politik und Sicherheit
Hauptabteilung Analyse und Beratung
T +49 30 / 26 996-3460
ferdinand.gehringer@kas.de

Postanschrift: Konrad-Adenauer-Stiftung, 10907 Berlin

Herausgeberin: Konrad-Adenauer-Stiftung e. V., 2024, Berlin
Gestaltung: yellow too, Pasiek Horntrich GbR
Satz: Franziska Faehnrich

Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-98574-240-0