November 2021 · Dr. Sven Herpig

Cybersicherheit und die Volksrepublik China

Ein Überblick aus deutscher Perspektive

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Inhalt

1. Einleitung

Die 5G-Debatte der vergangenen Jahre[1] hat einmal mehr verdeutlicht, dass Technologiepolitik aus unterschiedlichen Elementen besteht, die zusammengeführt werden müssen, um gute Policies zu ermöglichen. Bei 5G gehört dazu nicht nur das technische Verständnis darüber, wie die Technologie funktioniert, sondern auch nachrichtendienstliche Erkenntnisse sowie geopolitische Analysen. Während die deutsche Debatte durch gute technische Studien zu 5G[2] und langjährige nachrichtendienstliche Arbeit zur Volksrepublik China[3] angereichert werden konnte, wurde die geopolitische Perspektive oft eher stiefmütterlich behandelt. Es wurde versäumt, die 5G-Debatte zu nutzen, um Deutschlands Position – und natürlich auch die der Europäischen Union – gegenüber einer technologisch aufstrebenden Volksrepublik China zu definieren.[4]

Einer solchen Positionierung geht ein besseres Verständnis der jeweiligen Thematik voraus. Das gilt daher auch für die chinesische Cybersicherheitspolitik, mit der man sich weitaus intensiver auseinandersetzen muss, als es in der Vergangenheit getan wurde. Während es im Ausland bereits Institutionen gibt, die dies stark vorantreiben[5], fällt die deutsche Debatte bei Cybersicherheit oft in alte Denkmuster zurück: digitale Unabhängigkeit von den Vereinigten Staaten sowie die Bekämpfung von Russland als Beeinflusser von Wahlen und sichere Zuflucht für Cyberkriminelle. Während beides relevante Aspekte für die Sicherheitspolitik Deutschlands darstellen, fehlt es weiterhin an einer grundsätzlichen, interdisziplinären Betrachtung von chinesischer Cybersicherheitspolitik und deren Auswirkungen auf Deutschland.

Erste Anhaltspunkte, warum gerade die Cybersicherheitspolitik ein Politikfeld ist, mit dem sich deutsche Expert:innen auseinandersetzen sollten, sind in der im August 2021 veröffentlichten bitkom-Studie zu finden[6]. Demnach ist China nach Russland die zweitgrößte ausländische Cyberbedrohung für die deutsche Wirtschaft. Gemäß dem Motto „There are only two types of companies – those that know they've been compromised, and those that don't know"[7] und einer Unklarheit über die jeweilige Zurechnungsfähigkeit der befragten Firmen und ihrer Dienstleister, sollten diese Zahlen natürlich mit Vorsicht betrachtet werden. Dennoch handelt es sich hierbei um eine interessante Erkenntnis. Zusätzlich warnte auch der Verfassungs-

1 wid/sto (2021), Wenig Beifall für das geplante IT-Sicherheitsgesetz 2.0, Deutscher Bundestag
2 Jan-Peter Kleinhans (2019), Whom to trust in a 5G world?, Stiftung Neue Verantwortung
3 Zum Beispiel: Bundesministerium des Innern (2001), Verfassungsschutzbericht 2000, Bundesministerium des Innern
4 High Representative of the Union for Foreign Affairs and Security Policy (2019), EU-China – A strategic outlook, European Commission
5 Zum Beispiel: Center for Security and Emerging Technology (2021), China Archives, Georgetown University und Citizen Lab (2021), China, University of Toronto
6 Achim Berg und Sinan Selen (2021), Wirtschaftsschutz 2021, bitkom
7 Michael Joseph Gross (2011), Enter the Cyber-Dragon, Vanity Fair

schutz zuletzt vor Cyberoperationen der Gruppe APT 31 gegen öffentliche Stellen.[8] Die Gruppe wird der Volksrepublik China zugerechnet. Im Juli 2021 verurteilte eine internationale Koalition von Staaten, inklusive der Europäischen Union, das Verhalten der Volksrepublik China im Cyberraum als unverantwortlich.[9] APT 31 war eine der beiden Gruppen, deren Aktivitäten zu dieser scharf formulierten Erklärung führten. Dies ist aber nur eine Seite der Medaille, denn gleichzeitig ist die Gefährdungslage für die Volksrepublik China im Cyberraum nach wie vor hoch[10], weshalb Regulierungen im Bereich der Cyber- und Informationssicherheit in den vergangenen Jahren stark vorangetrieben wurden[11].

Das ausgegebene Ziel der Volksrepublik China – was den Stellenwert der Cybersicherheitspolitik nochmals unterstreicht – ist es, eine „cyber great power" (网络强国) zu werden.[12] Das Verständnis der aktuellen Lage, Aktivitäten und Bestrebungen des Landes im Cyberraum ist daher eine notwendige Bedingung für gute Cybersicherheitspolitik. Im Folgenden wird ein erster kurzer Überblick über diese Facetten der Cybersicherheitspolitik der Volksrepublik China gegeben.

8 Bundesamt für Verfassungsschutz (2021), BfV Cyber-Brief Nr. 01/2021, Bundesamt für Verfassungsschutz
9 The White House (2021), The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, The White House
10 Vgl z. B. CNCERT/CC (2020), 2020 Annual Report, CNCERT/CC und Thomas Brewster (2021), Exclusive: An American Company Fears Its Windows Hacks Helped India Spy On China And Pakistan, Forbes und Bundeskriminalamt (2019), Bundeslagebild Cybercrime 2018, Bundeskriminalamt und Bundeskriminalamt (2011), Bundeslagebild Cybercrime 2010, Bundeskriminalamt
11 Siehe Abschnitt 3.
12 Dakota Cary (2021), China's National Cybersecurity Center, Center for Security and Emerging Technology und Rogier Creemers, Graham Webster, Paul Triolo, Katharin Tai, Lorand Laskai, und Abigail Coplin (2018), Lexicon: 网络强国 Wǎngluò Qiángguó, New America

2. Die Volksrepublik China als Threat Actor für Deutschland

Im Rahmen des Aspen Cyber Summits Ende September 2021 beschrieb Rob Joyce, Leiter der Cybersicherheitsabteilung der National Security Agency, die Cyberfähigkeiten der Volksrepublik China wie folgt: „Scope and scale, China's off the charts. The amount of Chinese cyber actors dwarfs the rest of the globe, combined."[13]

Aus deutscher Perspektive lässt sich die Betrachtung der Volksrepublik China als Bedrohungsakteur in sechs Bereiche gliedern: 1. Überwachung von Minderheiten, Dissident:innen, Journalist:innen und Aktivist:innen, 2. Wirtschafts- und Konkurrenzspionage, 3. politische Spionage, 4. Kriminalität, 5. Subversion und 6. militärische Cyberoperationen. Es ist wichtig zu betonen, dass die Volksrepublik China nicht monolithisch ist und nicht alle Gruppen, die Cyberkampagnen aus der Volksrepublik durchführen, dies notwendigerweise im Auftrag der politischen Führung des Landes tun.[14] Analysen zeigen jedoch, dass die aktivsten Gruppen eine Verbindung zum Staat haben[15] und damit nicht explizit gegen die Interessen des Staates beziehungsweise einzelner Ministerien handeln. Dies verortet sie, spätestens wegen fehlender Sorgfaltspflicht, im staatlichen Verantwortungsbereich.[16] Möglicherweise auch deswegen ist vereinzelt zu beobachten, dass die Nutzung von Verschleierungstaktiken sowie die Zusammenarbeit der Gruppen untereinander und mit Dritten zunimmt. Diese Beobachtungen zeigen eine relevante Entwicklung bei den Cyberkampagnen, die Gruppen aus der Volksrepublik China zugerechnet werden. [17]

2.1. Überwachung

Die staatliche Überwachung der in der Volksrepublik China lebenden Menschen ist weitreichend dokumentiert.[18] Auch vor Ländergrenzen macht diese Überwachung nicht halt. Im Ausland lebende Tibeter:innen, Uigur:innen, Journalist:innen, Dissident:innen und Aktivist:innen sind Ziel von Überwachungsmaßnahmen im

13 Catalin Cimpanu (2021), Quote from Rob Joyce, Twitter
14 Richard J. Harknett und Max Smeets (2020), Cyber campaigns and strategic outcomes, Journal of Strategic Studies
15 Richard J. Harknett und Max Smeets (2020), Cyber campaigns and strategic outcomes, Journal of Strategic Studies
16 Jason Healey (2011), Beyond Attribution: Seeking National Responsibility for Cyber Attacks, Atlantic Council
17 Jack Goldsmith und Robert D. Williams (2018), The Failure of the United States' Chinese-Hacking Indictment Strategy, LAWFARE und Catalin Cimpanu (2021), Chinese hacking group APT31 uses mesh of home routers to disguise attacks, The Record und Patrick Howell O'Neill (2021), Chinese hackers disguised themselves as Iran to target Israel, Technology Review und Yonah Jeremy Bob (2021), China hacks Israel, Iran, for info on tech, business advances, The Jerusalem Post und Catalin Cimpanu (2021), Sprawling cyber-espionage campaign linked to Chinese military unit, The Record und FireEye (2014), SUPPLY CHAIN ANALYSIS: From Quartermaster to SunshopFireEye, FireEye und Josh Ye (2021), US-China tech war: who is the little-known Chinese firm in the crosshairs of US for alleged cyberattacks?, South China Morning Post
18 Zum Beispiel: World Report 2020 (2020), China's Global Threat to Human Rights, Human Rights Watch und The Citizen Lab (2021), China Archives, University of Toronto

Cyberraum aus der Volksrepublik China.[19] Eine entsprechende Überwachung, unabhängig vom physischen Ort, an dem sich die Menschen befinden, hat anscheinend einen hohen Stellenwert in der Prioritätenliste der Volksrepublik China. Ein Beispiel dafür ist, dass eine Gruppe, die der Volksrepublik China zugeordnet wird, eine Reihe an hochwertigen Schwachstellen und Exploits dazu genutzt hat, Smartphones von Uigur:innen mit Schadsoftware zu infizieren.[20] Daraus ergibt sich, dass in Deutschland lebende Minderheiten wie etwa Uigur:innen und Aktivist:innen, aber auch Student:innen[21] zu den Zielen chinesischer Überwachungsoperationen im Cyberraum gehören können. Gespräche mit Betroffenen bestätigen diese Bewertung. Dabei sind E-Mail-Accounts ein häufiger Angriffsziel; Messenger und soziale Medien werden als Kanäle für Anbahnung und Überwachung genutzt. Entsprechende Aktivitäten finden vermehrt zu Zeiten relevanter geopolitischer Ereignisse statt, zum Beispiel der Proteste in Hong Kong.

Polizeien, Verfassungsschutzbehörden oder Cybersicherheitsinstitutionen auf Länderebene sollten Beratungsangebote im Bereich IT-Sicherheit und Überwachung anbieten und proaktiv auf die Diaspora zugehen, sowie Sprach- und Kulturkenntnisse auf beiden Seiten ausbauen, um die Cybersicherheit der betroffenen Gruppen zu erhöhen. Der Austausch kann darüber hinaus auch zum besseren Verständnis der Behörden über die Aktivitäten der Volksrepublik China beitragen.

2.2. Wirtschafts- und Konkurrenzspionage[22]

Seit gut zwei Jahrzehnten führt die Volksrepublik China wirtschaftliche und politische Spionage im Cyberraum in verschiedenen Ländern durch.[23]

Dabei wird in Deutschland in Bezug auf die Volksrepublik China oftmals von Industriespionage gesprochen. Die angeführte bitkom-Studie[24] zeigt, welche Aktualität diese Herausforderung weiterhin hat. Ein weiteres Beispiel ist die Winnti-Kampagne (APT 41). 2019 veröffentlichten Journalist:innen des Bayerischen Rundfunks und des Norddeutschen Rundfunks eine umfassende Recherche zu einer groß angelegten

19 Unter anderem: Mike Dvilyanski and Nathaniel Gleicher (2021), Taking Action Against Hackers in China, Facebook und Eli Clemens (2021), Evil Eye Gazes Beyond China's Borders: Troubling Trends in Chinese Cyber Campaigns
20 Ian Beer (2019), A very deep dive into iOS Exploit chains found in the wild, Google Project Zero und Apple (2019), A message about iOS security, Apple und Alex Hern (2019), Uighurs in China were target of two-year iOS malware attack – reports, The Guardian und Patrick Howell O'Neill (2021), How China turned a prize-winning iPhone hack against the Uyghurs, Technology Review
21 Human Rights Watch (2021), How China's Long Reach of Repression Undermines Academic Freedom at Australia's Universities, Human Rights Watch
22 Bundesamt für Verfassungsschutz (2021), Chinas neue Wege der Spionage, Bundesamt für Verfassungsschutz
23 Richard J. Harknett und Max Smeets (2020), Cyber campaigns and strategic outcomes, Journal of Strategic Studies
24 Achim Berg und Sinan Selen (2021), Wirtschaftsschutz 2021, bitkom

Kampagne mit mutmaßlich chinesischem Ursprung.[25] Bei diesem Vorfall handelte es sich um Wirtschafts- und Konkurrenzspionage gegen Unternehmen, darunter Bayer, Thyssen-Krupp, BASF, Henkel und Siemens. Bereits 2014 beziehungsweise 2016 – dazu gibt es widersprüchliche Aussagen – wurde das deutsche Unternehmen TeamViewer Ziel einer Cyberoperation mittels Winnti-Schadsoftware.[26] Da die TeamViewer-Software unter anderem für Fernwartung genutzt wird, ist es möglich, dass es sich hierbei um eine gezielte Kompromittierung der Lieferkette handelte, um in IT-Systeme anderer Akteure einzudringen. Auch im Rahmen der Operation Cloudhopper, die auf die Lieferkette abzielte[27], waren vermutlich deutsche Unternehmen das Ziel der Gruppe APT 10, die der Volksrepublik China zugerechnet wird.[28] Auch deutsche Unternehmen, die in der Volksrepublik tätig sind, können Ziel entsprechender Aktivitäten werden. So warnt das Bundesamt für Verfassungsschutz vor der Schadsoftware GoldenSpy, die bei der Installation der verpflichtenden Steuersoftware IntelligentTax nachgeladen wurde.[29]

Diese Beispiele fügen sich nahtlos in die von der Bundesregierung kritisierte „Industriespionage im großen Stil" der Volksrepublik China ein, deren Ziel vor allem die Unterstützung der „Made in China 2025"-Strategie[30] und des jeweils aktuellen Fünf-Jahres-Plans[31] ist.[32] Von Wirtschafts- und Konkurrenzspionage in Deutschland sind daher vor allem Bereiche betroffen, in denen Unternehmen in der Volksrepublik China noch Aufholbedarf haben und deutsche Unternehmen führend sind. Diese Bereiche werden allerdings zunehmend weniger.[33] Relevant sind in diesem Kontext jedoch auch Forschungseinrichtungen, in denen an Spitzentechnologie geforscht wird, und die aus diesem Grund Ziel von Wirtschafts- und Konkurrenzspionage werden können.[34]

25 Hakan Tanriverdi, Svea Eckert, Jan Strozyk, Maximilian Zierer und Rebecca Ciesielski (2019), Angriff auf das Herz der deutschen Industrie und Bundesamt für Verfassungsschutz (2019), BfV Cyber-Brief Nr. 01/2019, Bundesamt für Verfassungsschutz

26 Marcel Rosenbach (2019), Wie Hacker aus Fernost Teamviewer ausspionierten, SPIEGEL Online und Catalin Cimpanu (2019), Chinese cyberspies breached TeamViewer in 2016, ZDNet

27 Bundesamt für Sicherheit in der Informationstechnik (2018), Die Lage der IT-Sicherheit in Deutschland 2018, Bundesamt für Sicherheit in der Informationstechnik

28 rtr (2018), China hat offenbar Hacker für Angriffe auf IBM und HPE beauftragt, Handelsblatt und Bundesamt für Verfassungsschutz (2017), BfV Cyber-Brief Nr. 2/2017, Bundesamt für Verfassungsschutz

29 Bundesministerium des Innern, für Bau und Heimat (2021), Verfassungsschutzbericht 2020, Bundesministerium des Innern, für Bau und Heimat

30 Staatsrat der Volksrepublik China (2015), 国务院关于印发《中国制造2025》的通知 (Ankündigung des Staatsrates zur Veröffentlichung von „Made in China 2025"), Staatsrat der Volksrepublik China

31 Compilation and Translation Bureau (2016), Central Committee of the Communist Party of China, The 13th Five-Year-Plan for economic and social development of the People's Republic of China (2016-2020), National Development and Reform Commission und Xinhua (2021), 中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要 (14. Fünf-Jahres-Plan für die politische und soziale Entwicklung der Volksrepublik China und langfristige Ziele für das Jahr 2035), Xinhuanet

32 Dana Heide und Christof Kerkmann (2019), Berlin verdächtigt Chinas Regierung der Industriespionage im großen Stil, Handelsblatt und Bundesministerium des Innern, für Bau und Heimat (2021), Verfassungsschutzbericht 2020, Bundesministerium des Innern, für Bau und Heimat

33 apr/Reuters (2021), Chinesische Maschinenbauer hängen deutsche Konkurrenten immer weiter ab, Spiegel Online

34 Zum Beispiel Richard Pérez-Peña (2013), Universities Face a Rising Barrage of Cyberattacks, The New York Times und Federal Bureau of Investigation (2019), CHINA: THE RISK TO ACADEMIA, Federal Bureau of Investigation

2.3. Politische Spionage

Deutschland ist jedoch nicht nur von Wirtschafts- und Konkurrenzspionage aus der Volksrepublik China betroffen, sondern auch von politischer Spionage. Natürlich ist politische Spionage im Cyberraum gegen Deutschland kein Alleinstellungsmerkmal der Volksrepublik China. Während zum Beispiel die Snowden-Veröffentlichungen amerikanische Spionage gegen Deutschland belegt haben[35], wurde unter anderem der Deutsche Bundestag Ziel von politischer Spionage durch Russland[36].

Internationales Aufsehen erregte zuletzt das Vorgehen chinesischer Gruppen, insbesondere von APT 31 und APT 40 , aber auch weiteren Gruppen wie APT 41[37], bei der Ausnutzung von Schwachstellen in Microsoft Exchange Servern weltweit. Im Vergleich zu anderen Kampagnen, wie der Russland zugerechneten Cyberoperation gegen Ziele auf der ganzen Welt mittels einer Kompromittierung von SolarWinds[38], bezeichnete IT-Sicherheitsexperte Dmitri Alperovitch das chinesische Vorgehen als „indiscriminate, disruptive, untargeted“[39]. Dies widerspricht der klassischen Vorstellung und Toleranz von Spionageoperationen.

Ziele politischer Spionageoperationen aus der Volksrepublik China sind unter anderem „personally identifiable information (PII) and sensitive government documents“.[40]

Im Cyber-Brief des Bundesamtes für Verfassungsschutz, veröffentlicht im Januar 2021, heißt es, dass öffentliche Stellen in Deutschland Ziel von Aufklärungsaktivitäten und Angriffsvorbereitungshandlungen der Gruppe APT 31 geworden sind.[41] Bei APT 31, auch als Zirconium oder Judgment Panda bezeichnet, handelt es sich um einen Akteur, der dem chinesischen Verantwortungsbereich zugeschrieben wird.[42] In Deutschland sind im Bereich der politischen Spionage zusätzlich APT 15 und APT 25 aktiv.[43] Ziel dieser Gruppen ist „dabei mutmaßlich die Ausspähung politischer Handlungsstrategien, Verhandlungspositionen und Inhalte sowie Fortschritte politischer Entscheidungsfindung“.[44]

35 Zum Beispiel wid (2015), Ergebnisse des NSA-Ausschusses im Plenum gegensätzlich bewertet, Deutscher Bundestag
36 Zum Beispiel Florian Flade und Georg Mascolo (2020), Bärenjagd, Süddeutsche Zeitung
37 Matthieu Faou, Mathieu Tartare und Thomas Dupuy (2021), Exchange Server werden von mindestens 10 APT-Gruppen angegriffen, welivesecurity by eset
38 Patrick Beuth (2020), Der Spionagefall des Jahres, SPIEGEL Online
39 Bradley Barth (2021), Is US muddling its cyber policy by policing China and Russia differently?, SC Media
40 intrusiontruth (2021), An (in)Competent Cyber Program – A brief cyber history of the ‘CCP’, intrusiontruth
41 Bundesamt für Verfassungsschutz (2021), BfV Cyber-Brief Nr. 01/2021, Bundesamt für Verfassungsschutz
42 FireEye (2021), Die Hackergruppen hinter Advanced Persistent Threats, FireEye
43 Bundesministerium des Innern, für Bau und Heimat (2021), Verfassungsschutzbericht 2020, Bundesministerium des Innern, für Bau und Heimat und Bundesministerium des Innern, für Bau und Heimat (2020), Verfassungsschutzbericht 2019, Bundesministerium des Innern, für Bau und Heimat und Bundesamt für Verfassungsschutz (2020), BfV Cyber-Brief Nr. 1/2020, Bundesamt für Verfassungsschutz
44 Bundesministerium des Innern, für Bau und Heimat (2021), Verfassungsschutzbericht 2020, Bundesministerium des Innern, für Bau und Heimat

2.4. Kriminalität

Auch im Bereich Cyberkriminalität sind der Volksrepublik China zugeordnete Gruppen, zum Beispiel APT 41, aktiv.[45] Dazu gehört neben dem Kopieren von Daten, das Ausrollen von Erpressungssoftware und Software zum Minen von Kryptowährung.[46] In 2020 beschrieb der amerikanische Generalstaatsanwalt Jeffrey A. Rosen dieses Vorgehen als geplant und strukturell, in dem er sagte, „[r]egrettably, the Chinese communist party has chosen a different path of making China safe for cybercriminals [...]".[47] Aus den Stellungnahmen des amerikanischen Justizministeriums[48] und des Weißen Hauses[49] ergibt sich, dass sowohl der Volksrepublik China zugeordnete Gruppen – während ihrer regulären Arbeitszeit und nebenberuflich („Moonlighting") – als auch beauftragte Dritte, kriminelle Aktivitäten gegen Akteure in anderen Staaten im Cyberraum durchführen. Zur Überschneidung von kriminellen und nachrichtendienstlichen Aktivitäten, zum Beispiel über Dienstleister (APT 3, APT 18, APT 17), APT-Boutiquen oder einfach als Diversifikation des Geschäftsmodells (APT 41), berichtete das Bundesamt für Sicherheit in der Informationstechnik mit Verweis auf externe Quellen in seinem Lagebild 2017.[50] Dabei handelt es sich sowohl um eine Vermischung der Akteure als auch von deren Werkzeugen und Techniken.[51]

Sieht man von Datenextraktionen im Rahmen von Wirtschafts- und Konkurrenzspionage ab, ist für Deutschland wenig über kriminelle Aktivitäten – zum Beispiel Ausrollen von Erpressungssoftware – seitens der Volksrepublik China zugeordneten Gruppen bekannt.[52] Lediglich im Lagebericht zur IT-Sicherheit in Deutschland 2014 wird ein Social-Engineering-Fall bei Großkonzernen beschrieben, bei dem die Kriminellen EC-Karten samt PIN ihrer Ziele – hochrangige Mitarbeiter von Großkonzernen – in die Volksrepublik China haben schicken lassen.[53]

45 The White House (2021), The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, The White House

46 The White House (2021), The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, The White House

47 The United States Department of Justice (2020), Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally, U.S. Department of Justice

48 The United States Department of Justice (2020), Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally, U.S. Department of Justice

49 The White House (2021), The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, The White House

50 Bundesamt für Sicherheit in der Informationstechnik (2017), Die Lage der IT-Sicherheit in Deutschland 2017, Bundesamt für Sicherheit in der Informationstechnik und intrusiontruth (2021), An (in)Competent Cyber Program – A brief cyber history of the 'CCP', intrusiontruth

51 Bundesamt für Sicherheit in der Informationstechnik (2016), Die Lage der IT-Sicherheit in Deutschland 2016, Bundesamt für Sicherheit in der Informationstechnik und intrusiontruth (2021), An (in)Competent Cyber Program – A brief cyber history of the 'CCP', intrusiontruth

52 Annahme basiert u. a. auf der Auswertung der Bundeslagebilder Cybercrime des Bundeskriminalamtes aus den Jahren 2010-2020 und den Berichten zur Lage der IT-Sicherheit in Deutschland des Bundesamtes für Sicherheit in der Informationstechnik aus den Jahren 2005-2020.

53 Bundesamt für Sicherheit in der Informationstechnik (2014), Die Lage der IT-Sicherheit in Deutschland 2014, Bundesamt für Sicherheit in der Informationstechnik

2.5. Subversion

Das Bundesamt für Verfassungsschutz stellt fest, dass „[b]esonders die Nachrichtendienste [...] der Volksrepublik China [...] Cyberangriffe [nutzen], um Informationen auf digitalem Weg zu beschaffen, politisch Einfluss zu nehmen oder Sabotage zu verüben“.[54] Jedoch werden keine konkreten Vorfälle genannt, in denen die Volksrepublik China, oder ihr zugeordnete Gruppen, in Deutschland Subversion durch Cyberoperationen, also zum Beispiel Einflussnahme auf den demokratischen Prozess, betrieben haben.

2.6. Militärische Operationen

Die Volksrepublik China verfügt im militärischen Bereich seit mehr als zehn Jahren über Cyberfähigkeiten.[55] Diese Fähigkeiten werden in unterschiedlichen Bereichen eingesetzt. Ein Beispiel dafür ist APT1, die der Volksbefreiungsarmee zugeordnet wird und Wirtschaftsspionage durchgeführt hat.[56] Über den Einsatz dieser Fähigkeiten im Rahmen von offensiven militärischen Cyberoperationen (OMCO)[57] gegen deutsche Ziele ist bisher nichts bekannt.

54 Bundesministerium des Innern, für Bau und Heimat (2021), Verfassungsschutzbericht 2020, Bundesministerium des Innern, für Bau und Heimat
55 The Times (2011), China admits training cyberwarfare elite unit, The Times
56 Mandiant (2013), APT1: Exposing One of China's Cyber Espionage Units, Mandiant
57 Matthias Schulze (2020), Militärische Cyber-Operationen, Stiftung Wissenschaft und Politik

3. Die Cybersicherheitspolitik der Volksrepublik China

„Ohne Cybersicherheit gibt es keine nationale Sicherheit“, verkündete der chinesische Präsident Xi Jinping 2018 bei einem Treffen der Arbeitsgruppe Cybersicherheit und Informatisierung[58]. Unter Xi hat das Thema Cybersicherheit in China an enormer politischer Bedeutung gewonnen und wird von ihm in öffentlichen Reden auch als fundamentale Stütze für das Wirtschaftswachstum durch „Informatisierung“, eine Art chinesische Industrie 4.0, dargestellt.

3.1. Cybersicherheit als nationale Priorität

Das Thema Cybersicherheit beschäftigt die chinesische Regierung spätestens seit 1994, als sie eine erste Verordnung zur Sicherheit von IT-Systemen veröffentlichte[59]. Es folgten weitere Gesetze, Regelungen und erste Standards, doch 2021 hat das Thema noch einmal an zusätzlicher Bedeutung gewonnen: Allein im Sommer dieses Jahres verabschiedete die chinesische Legislative das Datensicherheitsgesetz[60] und das Gesetz zum Schutz persönlicher Informationen[61]. Zusätzlich veröffentlichte die Cyberspace Administration of China (国家互联网信息办公室, CAC) eine neue Version der Regeln für das Cybersecurity Review[62]. Außerdem veröffentlichte das Ministerium für Industrie und Informationstechnik (中华人民共和国工业和信息化部, MIIT) zum ersten Mal eine Regulierung zum Umgang mit Sicherheitslücken[63] und einen Drei-Jahres-Plan zur Stärkung des chinesischen Cybersicherheitssektors[64]. Viele der öffentlich bekannten Maßnahmen sind eher dazu ausgelegt, die IT-Sicherheit in der Volksrepublik zu erhöhen.

Die politische Aufmerksamkeit auf höchster Ebene und die damit verbundene geschäftige Regulierungsarbeit hat seine Gründe. Seit Beginn des Breitbandausbaus

58 Cyberspace Administration of China (2018), 习近平：没有网络安全就没有国家安全 (Xi Jinping: Ohne Cybersicherheit gibt es keine nationale Sicherheit), Cyberspace Administration of China
59 Staatsrat der Volksrepublik China (1994), 中华人民共和国计算机信息系统安全保护条例 (Computer Information Systems Protection Regulations), The Central People's Government of the People's Republic of China
60 Nationaler Volkskongress der Volksrepublik China (2021), 中华人民共和国数据安全法 (Data Security Law of the People's Republic of China), Stanford University [Übersetzung]
61 Nationaler Volkskongress der Volksrepublik China (2021), 中华人民共和国个人信息保护法 (Personal Information Protection Law of the People's Republic of China), Stanford University [Übersetzung]
62 Cyberspace Administration of China (2021), 网络安全审查办法（修订草案征求意见稿）(Cybersecurity Review Measures (Revised, Draft for Comment)), Stanford University [Übersetzung]
63 Ministerium für Industrie und Informationstechnik (2021), 工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知 (Benachrichtigung zur Veröffentlichung der Regeln zum Umgang mit Schwachstellen in Netzwerkprodukten durch das Ministerium für Industrie und Informationstechnik, die Cyberspace Administration of China und das Ministerium für Öffentliche Sicherheit), Cyberspace Administration of China
64 Ministerium für Industrie und Informationstechnik (2021), 公开征求对《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》的意见 (Open Solicitation of Opinions on the Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry (2021-2023) (Draft for Solicitation of Opinions), Georgetown University [Übersetzung]

ist China technisch, vor allem auf der Hardware-Ebene, von US-amerikanischen und anderen ausländischen Herstellern abhängig[65]. Die Snowden-Veröffentlichungen bestätigten 2013 einige der schlimmsten Sorgen der chinesischen Regierung bezüglich der resultierenden Verwundbarkeit gegenüber US-amerikanischen Geheimdiensten. Zusätzlich betont die Regierung immer wieder, dass China selbst Ziel von Cyberkriminellen und Operationen ausländischer Staaten ist, was sich wiederum in wirtschaftlichen Schäden niederschlägt[66].

3.2. Chinas Gefährdungslage im Cyberraum

Bei allen politischen und kulturellen Unterschieden befasst sich auch die chinesische Regierung mit der gleichen Gefährdungslage im Cyberraum, wie jedes andere Land. Im November 2021 erklärten Offizielle des Ministeriums für Staatssicherheit (国安部, MSS), dass ausländische Nachrichtendienste die IT-Systeme chinesischer Fluggesellschaften kompromittiert hätten.[67] In seinem Lagebericht zur Cybersicherheit in China im Jahr 2020 berichtet das National Computer Network Emergency Response Technical Team/Coordination Center of China (国家计算机网络应急技术处理协调中心, CNCERT/CC) von Problemen mit ausländischen APTs with OceanLotus oder Rattlesnake, welche die gesellschaftliche Unsicherheit während der Covid19-Pandemie ausnutzen.[68] Darüber hinaus begegneten der dem CNCERT/CC auch teils Jahre alte, ungepatchte Sicherheitslücken wie HeartBleed, geleakte persönliche Daten in einem Großteil der WeChat-Miniprogramme, gigantische Botnetze, oder Aktivität von Ransomware-Gruppen in China[69]. Tatsächlich benennt das CNCERT/CC Deutschland zusammen mit den USA und den Niederlanden als eines der drei wichtigsten Hostländer, von denen aus Schadsoftware auf chinesischen Computern kontrolliert wird[70]. Besonders prominent ist in China das Problem geleakter und verkaufter Daten von Nutzer:innen aller möglichen technischen Dienste, für die es einen florierenden Schwarzmarkt gibt – von Internetbanking bis hin zu sozialen Medien[71]. Diese Probleme sind auch einer der wichtigsten Beweggründe für die chinesische Datenschutzgesetzgebung in den vergangenen Jahren, die besonders die Beziehung von Nutzer:innen und privaten Firmen ins Visier nimmt.

65 Zum Beispiel Nina Xiang (2021), Foreign dependence the Achilles' heel in China's giant tech sector, Nikkei Asia und Yu Hong (2017), Networking China, University of Illinois Press, S. 73
66 Zhuge Jianwei, Gu Lion, Duan Haixin und Taylor Roberts (2015), Investigating the Chinese Online Underground Economy, in: Jon R. Lindsay, Tai Ming Cheung und Derek S. Reveron (2015), China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, Oxford University Press
67 Catalin Cimpanu (2021), China says a foreign spy agency hacked its airlines, stole passenger records, The Record
68 CNCERT (2020), 2020 年我国互联网网络安全态势综述 (Zusammenfassung der Internet Netzwerksicherheitssituation in China 2020), CNCERT
69 CNCERT (2020), 2020 年我国互联网网络安全态势综述 (Zusammenfassung der Internet Netzwerksicherheitssituation in China 2020), CNCERT
70 CNCERT (2020), 2020 年我国互联网网络安全态势综述 (Zusammenfassung der Internet Netzwerksicherheitssituation in China 2020), CNCERT, S. 18
71 Zum Beispiel David Bandurski (2017), Cashing in on Dystopia, SupChina

Eine Gruppe von Forscher:innen schätzte 2015, dass der Schaden von Cyberkriminalität für die chinesische Wirtschaft im Jahr 2011 mehr als 5.36 Milliarden chinesische Yuan (etwa 706 Millionen Euro) betrug[72]. In Fällen, wo die Volksrepublik von Cyberkriminalität betroffen ist, reagiert die Regierung durchaus mit Strafverfolgung, wenn sich die entsprechende Gruppe innerhalb des Landes aufhält, wie zum Beispiel bei dem Mozi-Botnetz geschehen.[73]

3.3. Cybersicherheit versus 网络安全

Während in Deutschland und der EU tendenziell zwischen den Bereichen IT-Sicherheit/Informationssicherheit/Cybersicherheit und Datenschutz unterschieden wird, ist der chinesische Begriff für Cybersicherheit (网络安全, wörtlich: „Netzwerksicherheit“) deutlich breiter als der deutsche Begriff, sodass entsprechend betitelte Regulierungen oder Gesetze auch ein breites Spektrum an Themenbereichen enthalten können. Cybersicherheit in China beinhaltet einerseits klassische IT-Sicherheit, wie den Schutz Kritischer Infrastruktur oder die Prüfung von Hardware, die in kritischen Bereichen eingesetzt wird. Hinzukommen in China andererseits auch die weitgefasste „Informationssicherheit“ (信息安全), die je nach Definition auch „schädliche Informationen“ (有害讯息), wie Pornographie oder bestimmte politische Informationen beinhaltet, und Datensicherheit (数据安全), bei der es auch um den Schutz national relevanter und sensibler Daten abseits des Geheimschutzes geht[74]. Insgesamt sind die verschiedenen Bereiche nicht immer eindeutig voneinander zu trennen, sodass zum Beispiel auch Sicherheitsbedenken bezüglich der Veröffentlichung sensibler Informationen Datensicherheitspolitik motivieren können, die auf den ersten Blick auch deutscher Datenschutzpolitik ähneln könnte. Gleichzeitig ist auch Industriepolitik in China schon lange Cybersicherheitspolitik, da diese bereits seit Jahren maßgeblich darauf abzielt, Chinas Abhängigkeit von ausländischer Hardware, besonders im Bereich Kritische Infrastrukturen, zu verringern[75]. Auch das Konzept von „schädlichen Informationen“, deren Verbreitung die Regierung durch Maßnahmen wie Zensur gegebenenfalls einschränken sollte, kommt spätestens seit den späten 90er Jahren in China im Zusammenhang mit Cybersicherheit auf[76]. Es ist daher wichtig, die Herausforderungen und Ziele zu verstehen, mit denen chinesische Cybersicherheitspolitik sich befasst, und welche durchaus verschiede-

72 Zhuge Jianwei, Gu Lion, Duan Haixin und Taylor Roberts (2015), Investigating the Chinese Online Underground Economy, in: Jon R. Lindsay, Tai Ming Cheung und Derek S. Reveron (2015), China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, Oxford University Press

73 Catalin Cimpanu (2021), Mozi botnet authors arrested in China, The Record

74 „wichtige Daten“ (重要数据), s. Nationaler Volkskongress der Volksrepublik China (2021), 中华人民共和国数据安全法 (Data Security Law of the People's Republic of China), Artikel 21, Stanford University [Übersetzung]

75 Zum Beispiel Max Zenglein und Anna Holzmann (2019), Evolving Made in China 2025 - China's industrial policy in the quest for global tech leadership, MERICS

76 Staatskonzil der Volksrepublik China (1997, geändert 2011), 计算机信息网络国际联网安全保护管理办法 (Measures for Security Protection Administration of the International Networking of Computer Information Networks), Peking University [Übersetzung]

nen Motivationen hinter neuen Regulierungen stecken können. Dies ist besonders deswegen relevant, da sich die chinesische Regierung aktuell mitten in einem Prozess befindet, ein umfassendes Regulierungsregime für alle Bereiche zu verfassen, die mit dem Internet zusammenhängen, und in absehbarer Zeit weitere Regulierungen, Standards und Gesetze beschließen wird.

3.4. Chinas Cybersicherheitsarchitektur

Entsprechend der verschiedenen Bereiche und Zugänge zu Sicherheit gibt es auch in der chinesischen Bürokratie eine Reihe von Institutionen, die mehr oder weniger direkt mit verschiedenen Aspekten der Cybersicherheitspolitik befasst sind. Die wichtigsten Akteure sind das Ministerium für Öffentliche Sicherheit (公安部, MPS), das sich vor allem mit innerer Sicherheit beschäftigt und dem die chinesische Polizei untersteht, das MIIT, das MSS, und die CAC, die ursprünglich bei Internetregulierung zwischen den anderen Ministerien koordinieren sollte. Seit dem Abtritt des ersten CAC-Direktors Lu Wei wegen Korruptionsvorwürfen hat die CAC tendenziell an Einfluss über andere Ministerien verloren, besonders bei Themen wie Sicherheit. Sie ist unter anderem für inländische Zensur zuständig und taucht auch heute noch als koordinierende Agentur für breit angelegte Regulierungsinitiativen, wie einem Plan zur Regulierung von Algorithmen im September 2021, auf[77]. Hinzu kommen noch das Verteidigungsministerium und die Volksbefreiungsarmee, die lange maßgeblich für offensive Operationen im Cyberraum inklusive politischer und wirtschaftlicher Spionage zuständig war, diese Aufgaben jedoch in den letzten Jahren wohl zunehmend an das MSS abgetreten hat[78].

Unter der Schirmherrschaft der verschiedenen Ministerien gibt es außerdem eine Reihe an weiteren zuständigen Institutionen, wie das CNCERT/CC, das der CAC untergeordnet ist, Forschungsinstitute wie die China Academy for Information and Communication Technologies (dem MIIT untergeordnet), oder das Komitee TC260 (der CAC untergeordnet), welches für das Verfassen von technischen Standards, inklusive zu allen Aspekten der Cybersicherheit, zuständig ist. Hinzu kommt, dass sich in den Zuständigkeiten des MPS, MSS, CAC und MIIT jeweils eine Institution befindet, die für das Katalogisieren beziehungsweise Reagieren auf technische Schwachstellen zuständig ist.

77 Cyberspace Administration of China (2021), 关于印发《关于加强互联网信息服务算法综合治理的指导意见》的通 知 (Guiding Opinions on Strengthening Overall Governance of Internet Information Service Algorithms), Stanford University [Übersetzung]

78 intrusiontruth (2021), An (in)Competent Cyber Program – A brief cyber history of the 'CCP', intrusiontruth und zum Beispiel Insikt Group (2017), Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3, Recorded Future

Die überlappenden Zuständigkeiten der verschiedenen Institutionen führen auch in China durchaus zu innerbürokratischen Konflikten, die sich teils im Machtkampf um Zuständigkeiten in der Gesetzgebung niederschlagen. Ein Beispiel hierfür ist der Konflikt zwischen der CAC und dem MPS, die beide lange für sich beanspruchten, für Datensicherheit zuständig zu sein[79]. Ihre Zuständigkeiten sind auch in der finalen Version des Datensicherheitsgesetzes nicht eindeutig voneinander getrennt. Derartige Konflikte sorgen auch dafür, dass die verschiedenen Institutionen nicht unbedingt so nahtlos Informationen miteinander teilen, wie von der Zentralregierung vorgesehen.

Letzteres ist beispielsweise an den Ambitionen des Plans für das chinesische Sozialkreditsystem-Projekt 2015-2022 zu sehen, der unter anderem versucht, Behörden dazu zu bringen, mehr Informationen untereinander auszutauschen[80]. Inwieweit diese Konflikte sich auch bei Operationen im Ausland niederschlagen, ist schwer beurteilen.

Insgesamt herrscht im Bereich Cybersicherheit in China allerdings auch ein merklicher Fachkräftemangel. Die chinesische Regierung versucht, dieses Problem nun unter anderem durch die gezielte Aus- und Weiterbildung von Fachkräften im Bereich Cybersicherheit zu lösen. Ein Beispiel ist hier das neue Nationale Zentrum für Cybersicherheit in Wuhan, dessen erster Jahrgang 2022 mit zunächst etwa der Hälfte der anvisierten 2.500 Absolvent:innen seinen Abschluss erhält[81].

79 Samm Sacks, Qiheng Chen und Graham Webster (2020), Five Important Takeaways From China's Draft Data Security Law, New America
80 Xin Dai (2018), Toward a Reputation State: The Social Credit System Project of China, SSRN, S. 48
81 Dakota Cary (2021), China's National Cybersecurity Center - A Base for Military-Civil Fusion in the Cyber Domain, Georgetown University

4. Policy-Beispiel Schwachstellen-Regulierung: Fähigkeitsaufbau oder IT-Sicherheitsmaßnahme?

Die chinesische Cybersicherheitspolitik muss besser verstanden werden, damit die Auswirkungen der dort getroffenen politischen Entscheidungen für Deutschland besser beurteilt werden können. So wurde zum Beispiel im Juli 2021 in China eine neue Rechtsgrundlage zum Umgang mit Schwachstellen in „Netzwerk-Produkten" verabschiedet[82]. Es ist anzunehmen, dass die internationale Kooperation mit chinesischen IT-Sicherheitsforscher:innen zu Schwachstellen extrem stark eingeschränkt wird[83] und die neue Richtlinie zu einem Abschreckungseffekt führen wird. Jedoch ist es ohne weitere Informationen schwierig zu beurteilen, ob die Rechtsgrundlage a) den Zugriff auf unbekannte Schwachstellen verbessern und somit die Fähigkeiten der China zugeordneten Threat Actors erhöhen, b) das Problem der chinesischen Gefährdungslage adressieren oder c) zu beiden Aspekten beitragen soll.

Die Regulierung besagt unter anderem, dass Informationen über die Schwachstellen von Herstellern und Sicherheitsforscher:innen an das MIIT, genauer den Bereich Cybersecurity Threat and Vulnerability Information Sharing Platform, gemeldet werden sollen. Die Schwachstellen-Reports werden direkt an das National Network and Information Security Information Reporting Centre (国家网络与信息安全信息通报中心), das dem MPS untersteht, und das National Computer and Network Information Response Technological Handling and Coordination Centre (国家计算机网络应急技术处理协调中心), auch bekannt als CNCERT/CC, weitergeleitet. Weiterhin sollen die Hersteller in China umgehend andere Hersteller informieren, die im Rahmen der Lieferkette davon betroffen sein können (Up- and Downstream Supply Chain) und dafür sorgen, dass die Schwachstelle mitigiert wird. Erst im zweiten Schritt, innerhalb von zwei Tagen nach Kenntnis über die Schwachstelle, soll die Regierung informiert werden. Auch bei der Erkenntniserlangung durch IT-Sicherheitsforscher:innen steht im Vordergrund, dass keine Informationen über die Schwachstelle oder die Ausnutzung der Schwachstelle veröffentlicht werden sollten, bevor es mitigierende Maßnahmen und/oder Patches des Herstellers gibt. Es gibt hierbei jedoch Spielraum nach Absprache mit dem Hersteller, der Notifizierung des MPS und der Beurteilung durch das MIIT.

82 Ministerium für Industrie und Informationstechnik (2021), 工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知 (Benachrichtigung zur Veröffentlichung der Regeln zum Umgang mit Schwachstellen in Netzwerkprodukten durch das Ministerium für Industrie und Informationstechnik, die Cyberspace Administration of China und das Ministerium für Öffentliche Sicherheit), Cyberspace Administration of China

83 Catalin Cimpanu (2021), Chinese government lays out new vulnerability disclosure rules, The Record

Mit dem MPS ist quasi das chinesische Innenministerium direkt in die Meldekette von Schwachstellen involviert. Das CNCERT/CC teilt sich eine Adresse mit dem National Computer Network and Information Security Management Center (国家计算机网络与信息安全管理中心), das unter Verdacht steht, an der „Great Cannon“ beteiligt gewesen zu sein[84]. Außerdem dürfen IT-Sicherheitsforscher:innen ohne Absprache keine Informationen über die Schwachstelle an die Öffentlichkeit geben. Daher ist die Annahme des Zurückhaltens von Schwachstellen zur Erreichung geopolitischer Ziele nicht abwegig. Bereits in der Vergangenheit haben Akteure, die der Volksrepublik China zugeordnet werden, unbekannte Schwachstellen nicht gemeldet, sondern ausgenutzt, um zum Beispiel Uigur:innen zu überwachen.[85] In mindestens einem Fall[86] wurde eine Schwachstelle verwendet, die vorher bei dem weltbekannten chinesischen Hacking-Wettbewerb „Tianfu Cup“[87] (天府杯) von IT-Sicherheitsforscher:innen verwendet worden war. Der Tianfu Cup wurde sogar in die Nähe von Militärparaden gerückt, sozusagen als Äquivalent der Paraden im Cyberraum.[88]

Auf der anderen Seite sind jedoch auch das MIIT und die für Cybersicherheit zuständigen Akteure in den Schwachstellen-Prozess eingebunden. Dass keine Informationen über die Schwachstelle veröffentlicht werden sollen, bevor es mitigierende Maßnahmen oder Patches gibt, ergibt bis zu einem bestimmten Punkt auch Sinn. So werden zum Beispiel Informationen über unbekannte Schwachstellen, die von Google’s Project Zero gefunden werden, erst nach 90 Tagen veröffentlicht, wenn in dem Zeitraum vom Hersteller kein Patch bereitgestellt wird.[89] So soll den Herstellern ausreichend Zeit gegeben werden, Patches herzustellen, bevor böswillige Akteure mit den Informationen diese Schwachstellen ausnutzen können. Vor dem Hintergrund der aktuellen Gefährdungslage der Volksrepublik China im Cyberraum ist daher auch vorstellbar, dass mit der Regulierung Druck auf (inländische) Hersteller aufgebaut werden soll, damit unbekannte Schwachstellen schneller gepatched werden.

Um abschließend zu beurteilen zu können, welcher der beiden Wege, oder eine Mischung aus beiden, verfolgt wird, ist die Informationslage nicht ausreichend. Es bedarf einer genaueren Betrachtung, wie die Regulierung implementiert wird, gepaart mit IT-Sicherheitsanalysen zu zukünftigen chinesischen Aktivitäten, um herauszufinden, ob und wann die so gemeldeten Schwachstellen von der Volksrepublik zugeordneten Gruppen ausgenutzt werden.

84 Bill Marczak, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ron Deibert und Vern Paxson (2015), China’s Great Cannon, University of Toronto
85 Ian Beer (2019), A very deep dive into iOS Exploit chains found in the wild, Google und Zack Whittaker (2019), Sources say China used iPhone hacks to target Uyghur Muslims, TechCrunch
86 Patrick Howell O’Neill (2021), How China turned a prize-winning iPhone hack against the Uyghurs, Technology Review
87 Catalin Cimpanu (2021), Windows 10, iOS 15, Ubuntu, Chrome fall at China’s Tianfu hacking contest, The Record
88 J. D. Work (2021), China Flaunts Its Offensive Cyber Power, War on the Rocks
89 Project Zero (2021), Policy and Disclosure: 2021 Edition, Google

5. Empfehlung

Das Handeln der chinesischen Regierung ist nicht monolithisch. Ihre Cybersicherheitspolitik und -architektur müssen nuanciert betrachtet werden. Nur so kann ein entsprechendes Verständnis aufgebaut werden, das zu guten Regeln und Policies führt, die Deutschland im Cyberraum sicherer machen. Das ist auch deswegen notwendig, weil Deutschland in diesem Bereich von internationalen Partnerstaaten in Zukunft Entscheidungen abverlangt werden.[90] Analysen aktueller Entwicklungen mit Bezug zur Volksrepublik und der strategischen Prioritätensetzung des Landes können dazu beitragen, dass gefährdete Sektoren und Ziele in Deutschland besser identifiziert werden können, um so entsprechende Gegenmaßnahmen einzuleiten. Zusätzlich können die Analysen von Cyberoperationen der Volksrepublik dazu beitragen, die Ziele besser zu verstehen. Es geht also vornehmlich darum, Geopolitik auf der einen Seite und Cybersicherheitspolitik und IT-Sicherheit auf der anderen Seite zusammen zu bringen.

Trotz der Existenz von Policy- und Forschungseinrichtungen, die sich wahlweise mit Chinastudien, Cybersicherheitspolitik und IT-Sicherheit beschäftigen, gibt es bisher keinen Akteur in Deutschland, der diese Expertisenbereiche effektiv und interdisziplinär zusammenbringt. Das gilt mitunter auch für die Verbindung anderer Regionalstudien mit Cybersicherheitspolitik. Institutionen, die bereits diese unterschiedlichen Expertisenbereiche in ihrem Haus vereinen, sollten überlegen, diese zusammenzubringen. Ein entsprechender Akteur braucht jedoch sowohl strategische als auch operative Kompetenzen. Daher sollten Akteure, die einzelne dieser Bereiche abdecken, prüfen, ob eine entsprechende Kooperation – oder sogar eine institutionenübergreifende Lösung – lohnenswert sein kann. Parallel sollten Politik, Industrie und Philanthropie darüber nachdenken, entsprechende Fördermittel für unabhängige Policy-Forschung in diesem Bereich bereitzustellen.

90 Micah McCartney (2021), US defense bill may see Five Eyes swell to nine to counter China, Taiwan News

Über die Stiftung Neue Verantwortung

Die Stiftung Neue Verantwortung (SNV) ist ein gemeinnütziger Think Tank, der an der Schnittstelle von Technologie und Gesellschaft arbeitet. Die Kernmethode der SNV ist die kollaborative Entwicklung von Politikvorschlägen und -analysen. Die Expert:innen der SNV arbeiten nicht allein, sondern entwickeln und testen Ideen gemeinsam mit Vertreter:innen aus Politik und Verwaltung, Technologieunternehmen, Zivilgesellschaft und Wissenschaft. Unsere Expert:innen arbeiten unabhängig von Interessengruppen und Parteien. Unsere Unabhängigkeit gewährleisten wir durch eine Mischfinanzierung, zu der viele verschiedene Stiftungen, öffentliche Mittel und Unternehmensspenden beitragen.

Über den Autor

Dr. Sven Herpig ist Leiter für Internationale Cybersicherheitspolitik. Bei der SNV befasst Sven sich vorrangig mit der deutschen Cybersicherheitspolitik und -Architektur, staatlichem Hacken (u. a. dem „Bundestrojaner“) und IT-Schwachstellenmanagement, der staatlichen Beantwortung von Cyberoperationen, Angriffen auf Machine-Learning Anwendungen und Aktiver Cyberabwehr.

Der Autor bedankt sich bei den involvierten Expert:innen, Gesprächspartner:innen und Katharin Tai für die großartige inhaltliche Unterstützung, sowie bei Christina Rupp.

So erreichen Sie den Autor:

Dr. Sven Herpig
Leiter für Internationale Cybersicherheitspolitik
sherpig@stiftung-nv.de
+49 (0) 30 81 45 03 78 91
@z_edian

Impressum

Stiftung Neue Verantwortung e.V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Jan Klöthe