

Deutsche Lesefassung - Band 3

Cyberaufklärung und interner Streit über die China-Bewertung

CIA/FBI/NSA-Memorandum und zwei interne E-Mails

Grundlage: Vom Nutzer bereitgestellte, freigegebene Unterlagen der US-Regierung Stand der Übersetzung: 17. Juli 2026

Hinweise zu dieser Übersetzung

Diese Lesefassung übersetzt den lesbaren Inhalt dreier kurzer Dokumente. Geschwärzte Stellen erscheinen als [GESCHWÄRZT]; wiederkehrende Klassifizierungs-, Signatur- und Kontaktangaben werden zusammengefasst. Die Dokumente haben unterschiedlichen Charakter: Das erste ist ein Nachrichtendienstprodukt, die beiden anderen sind interne E-Mails. Die Neuformatierung ist keine amtliche Übersetzung.

Enthaltene Originaldokumente

1. CIA Wire Memo Summer 2020 DECLASS REDACTED.pdf, 1. Juli 2020, 2 Seiten 2. EMAIL_ICA.CommentsReMinorityView_30DEC2020_DECLASS REDACTED.pdf, 30. Dezember 2020, 2 Seiten 3. EMAIL_Everyone's favorite topic_23DEC2021_DECLASS REDACTED.pdf, 23. Dezember 2021, 1 Seite

1. Chinas Cyberaktivitäten als mögliche Vorstufe zur Wahlaufklärung

Übersetzter Originaltitel: Chinas Cyberaktivitäten sind wahrscheinlich eine Vorstufe zur Wahlspionage Originaldatei: CIA Wire Memo Summer 2020 DECLASS REDACTED.pdf Dokumentart: World Intelligence Review Dokumentnummer: WIRe2020-05063 Veröffentlichungsdatum: 1. Juli 2020 Gemeinsam erstellt unter Beteiligung von: CIA, FBI und NSA Originalumfang: 2 Seiten

Kernaussage

China sondierte den Präsidentschaftswahlkampf nach Möglichkeiten, seine Informationssammlung gezielt auszurichten und Erkenntnisse über politische Positionen zu amerikanisch-chinesischen Fragen zu gewinnen. Die amerikanische China-Politik hatte für Peking seit Langem hohe Priorität bei der Nachrichtengewinnung. Chinesische Cyberakteure hatten entsprechende Aktivitäten seit mindestens 2008 in jedem amerikanischen Präsidentschaftswahlkampf durchgeführt. [GESCHWÄRZTE QUELLENANGABEN] und offene Berichterstattung.

Chinesische Cyberakteure nahmen Informationen aus amerikanischen Präsidentschaftswahlkämpfen ins Visier, wahrscheinlich um Erkenntnisse zu gewinnen, die künftige Operationen ermöglichen könnten.

Zielpersonen und Vorgehensweise

Seit 2018 griffen chinesische Cyberakteure, die in der Privatwirtschaft als APT31 bekannt sind, persönliche E-Mail-Konten hochrangiger amerikanischer Führungspersonen an. Dazu gehörten Beamte im Exekutivbüro des Präsidenten, hochrangige Vertreter verschiedener Behörden der Exekutive, Mitglieder beziehungsweise Mitarbeiter des Kongresses und Angehörige der Bundesjustiz.

Seit 2017 arbeitete eine weitere [GESCHWÄRZTE STELLE] daran, unauffälligere Operationen zu ermöglichen. Dazu wurden die E-Mail-Adressen hochrangiger amerikanischer Amtsträger ermittelt und anschließend [GESCHWÄRZTE AKTEURE] beauftragt, die Passwörter der Zielkonten zu beschaffen oder zu knacken.

Im Vorfeld der Wahl 2020 stellte die Geheimdienstgemeinschaft fest, dass staatlich unterstützte chinesische Cyberakteure den Präsidentschaftswahlkampf des früheren Vizepräsidenten ins Visier nahmen. Wahrscheinlich sollten Informationen gesammelt werden, die spätere Operationen ermöglichen könnten. Nach dem Dokument war dies in diesem Wahlzyklus der erste beobachtete Fall, in dem diese Akteure einen amerikanischen Präsidentschaftswahlkampf unmittelbar angriffen.

China betrieb außerdem Cyberspionage gegen weitere Einrichtungen mit Wahlbezug. Die Geheimdienstgemeinschaft bewertete jedoch, dass China zu diesem Zeitpunkt nicht beabsichtigte, verdeckt einzugreifen, um den Wahlausgang zu beeinflussen. Die Aktivitäten könnten solche Operationen ermöglichen, falls Peking eine entsprechende Entscheidung trafe.

Spear-Phishing gegen einen Wahlkampf

Bis zum 20. Mai hatten APT31-Akteure Spear-Phishing-E-Mails mit Tracking-Links an Gmail-Konten von Beschäftigten eines Präsidentschaftswahlkampfs geschickt. Am 4. Juni gab Google öffentlich bekannt, dass APT31 den Wahlkampf angegriffen hatte.

Google und das FBI informierten die Verantwortlichen kurz nach Entdeckung der chinesischen Cyberoperationen. Vertreter von Google erklärten öffentlich, die Spear-Phishing-Versuche seien erfolglos gewesen.

Im Verlauf des vorausgegangenen Jahres sammelten chinesische Cyberakteure Informationen mit Wahlbezug aus amerikanischen Wählerdatenbanken, einem Unternehmen für Umfragedaten, politischen und gemeinnützigen Organisationen, Fundraising-Gruppen und Beratungsorganisationen politischer Wahlkämpfe.

Bedeutung der Tracking-Links

Die Methode von APT31, Tracking-Links zu versenden, deutete darauf hin, dass die chinesischen Akteure das Zielnetzwerk für spätere Schritte kartierten. Dazu könnte auch gehört haben, die E-Mail-Konten von Wahlkampfmitarbeitern im fernmeldeelektronischen Aufklärungssystem des chinesischen Militärs zur Sammlung vorzumerken.

Tracking-Links erfassen Metadaten wie Internetaktivitäten und Systeminformationen. Diese Informationen können verwendet werden, um Konten auszunutzen und weitere interessante Ziele zu bestimmen.

- Die Kenntnis des Betriebssystems und der Software eines Wahlkampfmitarbeiters würde Cyberakteuren zeigen, ob bekannte Schwachstellen schnell ausgenutzt werden könnten oder ob zunächst Schadsoftware für einen unbemerkten Zugang entwickelt werden müsste.
 - Öffnete eine Zielperson eine Spear-Phishing-E-Mail mit einem Tracking-Link, konnte dies selbst ohne Anklicken des Links bestätigen, dass das Konto aktiv war. Dadurch ließ sich die Zielauswahl für spätere Operationen möglicherweise eingrenzen.
-

2. FBI-Kommentare zur Minderheitsauffassung in der Wahlbewertung

Originalbetreff: ICA Comments Originaldatei:

EMAIL_ICA.CommentsReMinorityView_30DEC2020_DECLASS REDACTED.pdf Absenderin: Nikki L. Floris, Counterintelligence Division, FBI Datum: 30. Dezember 2020, 13:42 Uhr Originalumfang: 2 Seiten

Einleitung der weitergeleiteten Nachricht

Der Leiter der Election Threat Analysis beim National Intelligence Council leitete Kommentare des FBI zu [GESCHWÄRZTEM EMPFÄNGER ODER DOKUMENT] weiter. Der lesbare Text besagt, FBI-Direktor Christopher Wray habe [GESCHWÄRZTEN INHALT] bereits unterzeichnet. Weitere Teile der Einleitung sind geschwärzt oder nicht sicher lesbar.

Grundsätzliche Position des FBI

Nikki Floris übermittelte einige Gedanken zum aktualisierten Entwurf der Intelligence Community Assessment, die sich sämtlich auf die Minderheitsauffassung bezogen. Ein Teil der Einwände war dem Empfängerkreis nach ihrer Aussage bereits zuvor vom FBI-Team mitgeteilt worden.

Das FBI habe grundsätzlich nichts gegen die Aufnahme eines Textkastens mit der Minderheitsauffassung. Die darin enthaltene Analyse müsse jedoch denselben analytischen Standards entsprechen wie der übrige Bericht. Dies sei für das FBI eine „absolute rote Linie“.

Das FBI unterstützte außerdem nicht, die Minderheitsauffassung in die Kernaussagen aufzunehmen. Ohne angemessenen Kontext und Beschreibungen der Quellen werde die Minderheitsposition den übrigen Bewertungen der Geheimdienstgemeinschaft gleichgestellt. Im englischen Original steht an dieser Stelle offenbar das fehlerhafte Wort „parody“; aus dem Zusammenhang ergibt sich „parity“, also Gleichrangigkeit.

Einwand gegen die behauptete Absicht Chinas

Im ersten Absatz der Minderheitsauffassung hieß es, Chinas Führung habe auch „beabsichtigt“, mit einigen Aktivitäten Pekings mittelbar amerikanische Kandidaten und weitere Wahlbestandteile zu beeinflussen.

Die Geheimdienstgemeinschaft habe nach Aussage der E-Mail auf Grundlage eines größeren Erkenntnisbestands wiederholt festgestellt, es gebe keinen Beleg für eine solche Absicht. Wohl habe ein Bewusstsein bestanden, dass die Aktivitäten eine entsprechende Wirkung haben könnten.

Eine so eindeutige Behauptung der Absicht ohne stützende Belege sei nach Auffassung des FBI äußerst irreführend.

Gewichtung und Beschreibung der Quellen

Im zweiten Absatz erklärte der National Intelligence Officer, er gebe mehreren geheimdienstlichen und von Partnerdiensten stammenden Berichten größeres Gewicht. Die Minderheitsdarstellung enthalte jedoch keinerlei Beschreibung dieser Quellen.

Durch das Weglassen oder Verkürzen der Quellenbeschreibungen würden verdeckt gewonnene Meldungen amerikanischer oder verbündeter Dienste mit zweifelhafter Glaubwürdigkeit, schlecht nachvollziehbaren Quellenketten und kaum vorhandener Berichtshistorie ebenso gewichtet wie:

- Fernmeldeaufklärung zu identifizierten hochrangigen chinesischen Diplomaten und Nachrichtendienstvertretern;

- verdeckte Berichte über Entscheidungen in Peking aus Quellen mit belegter und im Allgemeinen zuverlässiger Berichtshistorie.

Einwand zur behaupteten Förderung von Protesten

Im letzten Aufzählungspunkt bewerte der National Intelligence Officer, China „könnte“ auch Proteste gefördert haben. Nach Auffassung des FBI gab es dafür in der Berichterstattung keine Belege. Auch die zugehörigen Quellenangaben stützten die Bewertung nicht.

Das FBI bezeichnete die Aussage als in hohem Maße irreführend und als falsche Wiedergabe der zugrunde liegenden Berichte.

Einwand gegen die Verwendung von Erkenntnislücken

Der Schlussabsatz der Minderheitsauffassung argumentierte, die Geheimdienstgemeinschaft habe Erkenntnislücken gerade bei jenen chinesischen Stellen, die wahrscheinlich Einflussoperationen durchführen würden.

Nach Auffassung des FBI erkannte diese Argumentation zunächst an, dass die vorhandene Sammlung Zurückhaltung der chinesischen Führung und keine Absicht zur Beeinflussung des Wahlausgangs gezeigt habe. Anschließend verlagere sie den Schwerpunkt auf Bereiche, in denen Erkenntnislücken mögliche Belege für die tatsächliche Durchführung übersehen haben könnten.

Dieser Wechsel sei mit früheren Teilen der Minderheitsargumentation unvereinbar und laufe darauf hinaus, die amerikanische Sammlung habe nicht gefunden, was China tatsächlich getan habe.

Das FBI wiederholte seine bereits zuvor vorgetragene Position: Die Abwesenheit von Belegen als Argument anzuführen, sei eine weitere „absolute rote Linie“.

Abschluss

Die Absenderin bedankte sich für die Arbeit und kündigte an, das FBI werde für weitere Entwürfe zur Verfügung stehen. Positiv hob sie hervor, dass die Änderungen im Iran-Abschnitt erheblich verbessert worden seien.

Sie wünschte ein gutes neues Jahr und verwies für den Folgetag auf eine Kollegin, da sie selbst nicht im Büro sein werde. Das Team werde am Montag wieder vollständig anwesend sein.

3. „Das Lieblingsthema aller“

Originalbetreff: Everyone's favorite topic Originaldatei: EMAIL_Everyone's favorite topic_23DEC2021_DECLASS_REDACTED.pdf Absender: National Intelligence Officer for Cyber
Originaldatum: 23. Dezember 2021 Originalumfang: 1 Seite

Der National Intelligence Officer for Cyber bat die Empfänger, einen neuen Bericht zu lesen.

Dieser Bericht berufe sich auf einige derselben Erkenntnisse und Argumentationsmuster, die 2020 verwendet worden seien, um zu erklären, bestimmte chinesische Einheiten seien nicht an Wahlbeeinflussung beteiligt gewesen, sondern hätten sich nur auf politische Sachfragen konzentriert.

Nun würden regionale Einflussaktivitäten und die Ausrichtung auf Sachthemen herangezogen, um zu begründen, dass China eine [GESCHWÄRZTE] Wahl beeinflusse. Als Belege würden teilweise dieselben Meldungen angeführt, welche die Mehrheitsanalyse 2020 in der Minderheitsbewertung zitiert habe.

Als Beispiel nenne der neue Bericht eine [GESCHWÄRZTE] Aktivität als Tätigkeit „des chinesischen Militärs“, obwohl die Geheimdienstgemeinschaft 2020 erklärt habe, der verantwortliche Akteur sei unbekannt gewesen.

Der Bericht beschreibe dieselbe Einheit, die [GESCHWÄRZTE PERSONEN] als an der Beeinflussung der US-Wahl 2020 beteiligt angesehen hätten. Nun werde sie als Einheit zur Wahlbeeinflussung bezeichnet und der chinesischen Regierung zugerechnet.

Der Absender schrieb, dieser Zufall sollte gegenüber den Aufsichtsgremien hervorgehoben werden. Es müsse geprüft werden, wie diese unterschiedliche Bewertung wirke und auf welcher logischen, nicht parteipolitischen Grundlage die Geheimdienstgemeinschaft solche Entscheidungen treffe.

Warum gelte dieselbe Einheit bei Aktivitäten in [GESCHWÄRZTEN LÄNDERN ODER WAHLEN] als an Wahlbeeinflussung beteiligt und als Förderer chinesischer Interessen, während dieselbe Tätigkeit in den Vereinigten Staaten als Einfluss auf Sachthemen, aber nicht als wahlbezogen bezeichnet werde?

Der abschließende Satz lautet hervorgehoben:

Es sind dieselben Personen, die dieselbe Art von Tätigkeit ausüben.

Dokumentenstatus und Übersetzungsvermerk

Das erste Dokument beschreibt beobachtete Cyberaufklärung und ihre mögliche Nutzung für spätere Operationen. Es hält zugleich fest, die damalige Bewertung habe keine chinesische Absicht zu einem verdeckten Eingriff in den Wahlausgang erkannt. Die beiden E-Mails dokumentieren einen internen Streit über Quellenqualität, analytische Standards und die Einordnung chinesischer Einflussaktivitäten. Sie sind keine eigenständigen Feststellungen über eine technische Manipulation von Stimmen.

Ende von Band 3