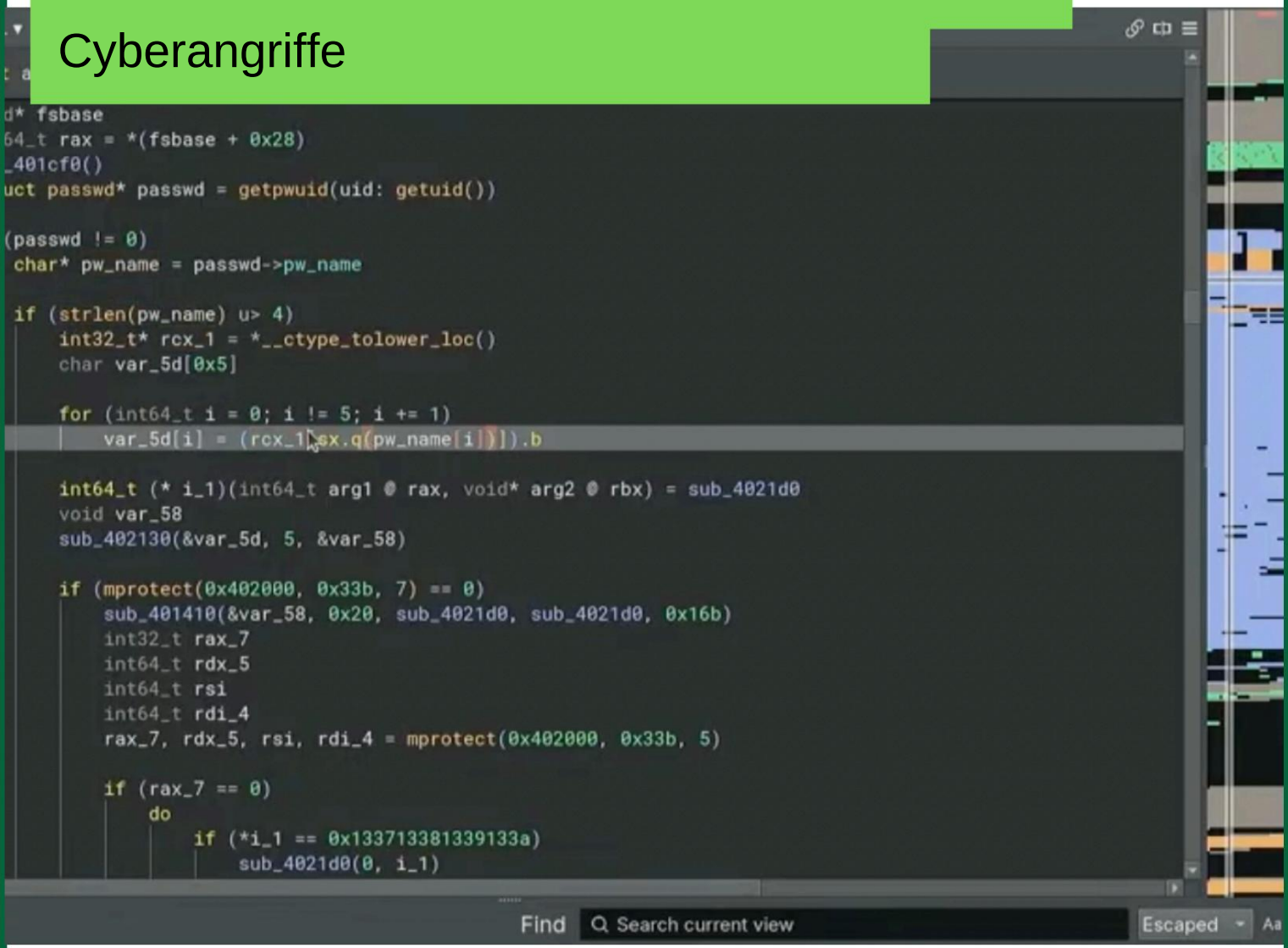
DARTMOUTH

ISTS

Vom **Chaos** zur **Leistungsfähigkeit**

Aufbau des US-Marktes für offensive Cyberangriffe



Winnona DeSombre Bernsen

Sergey Bratus

Bildnachweis: Screenshot des LiveCTF 2025-Finales bei DEFCON, https://www.youtube.com/watch?v=YcXgm9zy4Vk

EXECUTIVE SUMMARY

Die US-Regierung möchte im Cyberspace mit dem privaten Sektor zusammenarbeiten, um Bedrohungen in großem Maßstab zu bekämpfen. Derzeit fehlt jedoch ein schlüssiger öffentlicher Rahmen dafür. Will die US-Regierung die Unterstützung des privaten Sektors im offensiven Cyberspace stärken, müssen rechtliche und politische Änderungen vorgenommen werden, um kurzfristig realistische Möglichkeiten zu schaffen.

Im Oktober 2025 versammelte das Dartmouth Institute for Security, Technology and Society (ISTS) dreißig Experten aus Regierung, Industrie, Wissenschaft und Risikokapital nach den Chatham-House-Regeln, um zu analysieren, wie private Akteure die US-Regierung derzeit im Bereich „offensive Cyber“ unterstützen. Ziel war es, Empfehlungen zu erarbeiten, wie der private Sektor effektiv genutzt werden kann, um solche Aktivitäten auszuweiten. Offensive Cyber wurde weit gefasst und umfasste die Entwicklung von Tools, den Zugriff und die Generierung von Effekten für staatliche Cyberoperationen (OCO/CNE und Strafverfolgungsbehörden).

Die Diskussionsrunde ermittelte die folgenden drei Hauptergebnisse zur offensiven Cyber-Landschaft der USA:

1. **Die Dominanz im Cyberspace erfordert heute sowohl High- als auch Low-Equity-Fähigkeiten sowie opportunistischen Zugriff im großen Maßstab:** Ein Großteil der realen Cyber-Operationen erfordert keine neuartigen Zero-Day-Angriffe (High-Equity), sondern die opportunistische Ausnutzung von Fehlern des Gegners (Low-Equity). Unternehmen können enorme Gewinne erzielen, indem sie diese Fehler schnell erkennen und feststellen, welche Fehler einen auftragsbezogenen Zugriff ermöglichen.

2. **Der US-Privatsektor (durch staatliche Auftragnehmer, kleine Unternehmen und Einzelpersonen) unterstützt bereits aktiv Cyber-Operationen im Auftrag der US-Regierung.** Dies geschieht auf drei Arten: durch die Bereitstellung von Fähigkeiten (d. h. durch die Bereitstellung von Werkzeugen, Schulungen und Infrastruktur für Cyber-Operationen), durch die Bereitstellung von Zugang (d. h. durch das Eindringen in ein System und die Weitergabe des Zugangs an die Regierung) und durch die Erzielung eigener Effekte.

3. **Das Wachstum des privaten Sektors im Bereich offensiver Cyber-Tools und -Zugänge wird derzeit** durch die Art und Weise begrenzt, wie offensive Cyber-Technologien erworben werden: Private-Equity-Firmen investieren zwar in etablierte offensive Cyber-Unternehmen, junge Unternehmen erhalten jedoch wahrscheinlich keine privaten Investitionen, da Risikokapital normalerweise nicht in maßgeschneiderte Forschung oder Dienstleistungen investiert. Leider erwirbt die US-Regierung offensive Cyber-Fähigkeiten und -Zugänge größtenteils über Dienstleistungsverträge und Forschung.

Der Rundtisch identifizierte zwei Lücken und drei Chancen in diesem Bereich:

1. **Lücke:** Der Geheimdienst, das Militär und die Strafverfolgungsbehörden der Vereinigten Staaten sind optimiert für gezielte, eng gefasste Top-down-Operationen im Cyberspace. Dies führt jedoch nicht zu offensiven Cyber-Ergebnissen in dem von der US-Politik geforderten Tempo. Während der Privatsektor neue, zeitkritische Bottom-up-Möglichkeiten nutzen kann, die durch Fehler des Gegners entstehen, kann das operative Tempo der Regierung wahrscheinlich nicht mithalten.

2. **Chance:** Der US-Privatsektor ist bereit, offensive Cyber-Fähigkeiten und Zugang in größerem Umfang bereitzustellen, als derzeit genutzt wird. Es gibt Unternehmen, die über die

Das Unternehmen verfügt über die erforderlichen technischen Fähigkeiten, Werkzeuge und operativen Erfahrungen, um offensive Fähigkeiten und Zugriff bereitzustellen, und stellt der US-Regierung bereits Dienstleistungen zur Verfügung.

3. **Chance:** Auch private Akteure sind wahrscheinlich bereit, schnelle Cyber-Effekte zu erzielen
   Für die US-Regierung wäre dies ein Vorteil gegenüber begrenzten, weniger risikoreichen Zielen, erfordert aber zusätzliche Aufsicht sowie Haftungs- und Sicherheitsgarantien. Würde man solche Aktivitäten dem privaten Sektor überlassen, stünden den USA Ressourcen zur Verfügung, die sie auf Ziele mit höherer Priorität konzentrieren könnten.

4. **Lücke:** Der US-Regierung mangelt es an Transparenz, um eine klare Nachfrage nach offensivem Cyber-Schutz zu signalisieren.
   Während der Privatsektor im Auftrag der Regierung schnellere, zeitnahe und umfassendere Zugangsmöglichkeiten schaffen könnte, fehlt es der US-Regierung an klaren Möglichkeiten, diese Angebote zu fördern, und sie ist derzeit nicht in der Lage, klare Nachfragesignale zu senden.

5. **Chance:** Offensive Cyber-Maßnahmen erfordern heute ebenso viel Verständnis für Systeme wie
   Ausnutzung: Durchbrüche in der Software-Verständnisforschung und der Analyse offensiver Systeme durch die „Weird-Machine-Theorie“ der Cyber-Ausnutzung könnten es den USA ermöglichen, besser zu verstehen, wie sie gegnerische Systeme ausnutzen und gleichzeitig ihre eigenen verteidigen können.

Um den privaten Sektor bei offensiven Cyberangriffen wirksam einzusetzen, muss die US-Regierung Folgendes tun:

1. Entwicklung einer öffentlichen offensiven Cyber-Strategie;
2. Schaffung robuster Fähigkeitspipelines durch Pilotprogramme der NSA/des FBI/des Kriegsministeriums (DOW), Programme zur Innovationsforschung für kleine Unternehmen (SBIR), andere Transaktionsbehörden und nicht vertraglich gebundene Instrumente;
3. Investieren Sie in die Forschung zur offensiven Systemanalyse sowohl innerhalb akademischer Institutionen als auch private Cyber-Innovatoren; und
4. Genehmigung eines Pilotprogramms für Operationen des privaten Sektors gegen Akteure mit geringem Risiko.

Ein bundesweites Pilotprogramm gegen ausländische Kryptowährungsbetrüger und Ransomware-Betreiber könnte aus rechtlichen, operativen und Machbarkeitsgründen der beste erste Anwendungsfall sein – insbesondere angesichts des Wunsches der USA, die „Krypto-Hauptstadt der Welt“ zu werden, und des Nutzens, den die USA durch die Rückgewinnung von Vermögenswerten erzielen könnten, die das Land jährlich im Rahmen von Krypto-Betrug verlassen. Trotz der erfolgreichen Beschlagnahmung illegaler Kryptowährung im Wert von 15 Milliarden Dollar durch die Strafverfolgungsbehörden im Oktober 2025 deuten aktuelle Berichte darauf hin, dass Kryptowährung im Wert von über 75 Milliarden Dollar derzeit mit kriminellen Aktivitäten in Verbindung gebracht wird.

Offensive Cyber-Macht hängt nicht nur von der Entwicklung möglichst vieler Fähigkeiten und Zugänge ab, sondern auch von der Schaffung rechtlicher, finanzieller und institutioneller Rahmenbedingungen, die Innovationen verantwortungsvoll nutzen. Der Übergang vom Chaos zur Leistungsfähigkeit erfordert eine Umstellung von der Ad-hoc-Koordination auf ein strukturiertes Ökosystem: ein Ökosystem, das private Innovationen mit öffentlichen Zielen verbindet, rechtmäßige offensive Operationen des Bundes skaliert und die Führungsrolle der USA im Cyberspace bekräftigt.

Einleitung: Die Zukunft des offensiven Cyber

„Verteidigung und Angriff sind nicht gleichwertig. Die Verteidigung ist das Kind des Angriffs.“
- John Lambert

„Kein modernes Computersystem ist am Ende nur und genau das, was es sein soll.“
- Sergey Bratus

Offensive Cyberangriffe, wie auch immer sie definiert werden, werden sowohl als politische Idee als auch als technische Realität immer häufiger. Es bleibt jedoch unklar, was „offensive Cyberangriffe“ überhaupt bedeuten und welche Auswirkungen sie auf die wirtschaftliche und nationale Sicherheit der USA haben werden.

Nach den Chatham-House-Regeln ist Dartmouths Institut für Sicherheit, Technologie und Society (ISTS) versammelte eine Gruppe von dreißig Cyber-Experten aus den Bereichen Industrie, Wissenschaft, Think-Tanks, gemeinnützige Organisationen, Risikokapital und Regierung, um Folgendes zu diskutieren:

1. Wie unterstützt und führt der US-Privatsektor derzeit offensive Cyberoperationen für die US-Regierung durch?

2. Welche weiteren privaten und Investitionsmöglichkeiten gibt es im offensiven Cyberbereich?

3. Wenn die US-Regierung eine stärkere Zusammenarbeit mit dem privaten Sektor fördern möchte,
   Welche politischen und rechtlichen Änderungen könnten im Zusammenhang mit dem „offensiven Cyber“ vorgenommen werden, um kurzfristige und realistische Möglichkeiten zu schaffen?

Ausgangspunkt dieser Diskussionsrunde war die Annahme, dass die US-Politik zunehmend an einem privatwirtschaftlichen Ansatz interessiert ist, um auf die rasant steigende Zahl böswilliger Cyber-Akteure zu reagieren. Jüngste Maßnahmen des Kongresses1 und Erklärungen der US-Regierung23 zeigen deutlich, dass die US-Politiker trotz der Anerkennung der harten Arbeit sowohl des privaten als auch des öffentlichen Sektors der Ansicht sind, dass die derzeitigen Cyber-Optionen aufgrund mangelnder Geschwindigkeit, Flexibilität oder Reichweite letztlich unzureichend sind.4

Darüber hinaus verfolgen Cyber-Politiker in den USA5 sowie im Vereinigten Königreich, den Niederlanden, Japan und Kanada6 seit 2018 eine Strategie der Cyber-Persistenz (oder des anhaltenden Engagements).7 Die Theorie der Cyber-Persistenz legt Wert auf kontinuierliches Situationsbewusstsein im Cyberspace und die „anhaltende“ Auseinandersetzung mit dem Gegner in diesem Bereich.
Im Gegensatz zur Cyber-Abschreckung geht die Cyber-Persistenz davon aus, dass Nationalstaaten im Cyberspace ohne Angst vor einer Eskalation agieren können und dass die Interaktion zwischen Staaten, Unternehmen und Bürgern im Cyberspace auch im Krieg weiterhin wichtig ist.8 Der Übergang zu dauerhafteren, nicht

Die zunehmende Cyberaktivität eröffnet der US-Regierung die Möglichkeit, offensive Cyberangriffe als „zusätzlichen Pfeil im Köcher“9 hinzuzufügen (d. h. angemessen auf böswillige Akteure im Cyberspace zu reagieren), und zwar mithilfe einer Strategie, die wahrscheinlich eine stärkere und umfassendere Zusammenarbeit mit dem privaten Sektor erfordert.

Was dieses Dokument ist und was nicht

„Privatisierte offensive Cyber“ ruft oft unterschiedliche Definitionen, Autoritäten und Entsetzen hervor Geschichten aus der Cyber-Politik-Community sowie weitreichende Risiken und Kompromisse.
Dieses Dokument bietet keine umfassende Vision für alle Möglichkeiten, wie der private Sektor Cyber-Operationen durchführen könnte. Es handelt sich, vereinfacht und pragmatisch, um Folgendes:

1. Eine Analyse der aktuellen Lage für private Akteure, die offensive Cyber-Werkzeuge, Zugriffe und Auswirkungen für die US-Regierung;

2. Eine Auswahl der wichtigsten Chancen und Herausforderungen im Hinblick auf den aktuellen Stand der Dinge; und

3. Politische Empfehlungen, wie die USA die Rolle des privaten Sektors in offensive Cyber-Aktivitäten, einschließlich Fähigkeitsentwicklung, Zugangsentwicklung und Effektgenerierung.

Die offensive Cyber-Landschaft: Aktueller Stand der Dinge

A. Die Dominanz im Cyberspace erfordert heute sowohl hohe als auch niedrige Eigenkapitalkapazitäten sowie opportunistischen Zugang in großem Maßstab

Der Cyberspace hat sich weiterentwickelt: Die Software und Geräte, auf die wir heute angewiesen sind, unterscheiden sich grundlegend von denen vor 15 Jahren. So waren beispielsweise 2010 fast alle Geräte weltweit Desktop-Computer – heute machen mobile Geräte 60 % des globalen Marktanteils aus.
Darüber hinaus werden Systeme und Anwendungen immer komplexer: Containerisierung, Cloud-Umgebungen und weitläufige IT-Ökosysteme machen es jedem Unternehmen bekanntermaßen schwer, das digitale Terrain abzubilden und zu navigieren.11

Auch die Theorien zum offensiven Cyber-Schutz haben sich weiterentwickelt, um diesem neuen Komplex gerecht zu werden. Realität. Dies gilt insbesondere für hochentwickelte offensive Cyber-Funktionen wie Zero-Day-Exploits. Zero-Day-Exploits (d. h. das Ausnutzen von Zero-Day-Schwachstellen) wurden historisch als die Verwendung manipulierter Eingaben definiert, um die Ausführung von gegnerischem Code (oder „Bugs“) auf einem Opfercomputer zu ermöglichen.
In dieser Hinsicht wurde die Exploit-Entwicklung historisch als Suche nach *Primitiven* und deren zuverlässiger Zusammensetzung, *den Exploit-Ketten,* betrachtet.12 Dieses Verständnis geht jedoch davon aus, dass die Auswirkungen eines Exploit-Primitivs oder einer Exploit-Kette hervorstechen und daher leicht erkennbar sind.13 Heute können große Teile der eigenen, beabsichtigten Logik eines Zielsystems umfunktioniert werden, um Exploit-Ausführungen zu erstellen.

Engines – also „seltsame Maschinen“, die keine leicht erkennbaren Anomalien aufweisen: Solche Exploit-Ketten wurden bereits im Chrome-Browser von Google[14][15] und iMessage von Apple[16] gefunden . Die aufkommende „Seltsame-Maschinen-Theorie“ der Cyber-Exploitation, die ihren Ursprung in Dartmouth[17] hat, legt nahe, dass in jedem ausreichend großen System Exploits angenommen werden sollten. Mit anderen Worten: Anstatt ein Programm als eine Maschine zu betrachten, die möglicherweise Fehler enthält, ist jedes ausreichend komplexe Programm in Wirklichkeit eine Maschine mit endlosen „seltsamen Maschinen“, die nur darauf warten, von einem Angreifer entschlüsselt zu werden.[18]

Für manche Missionen werden immer seltene, versteckte und wertvolle Exploits sowie ungewöhnliche Maschinen erforderlich sein. Leider wird es immer teurer, diese Fähigkeiten zu entdecken und aufrechtzuerhalten.[19] Ein Teilnehmer des Dartmouth-Roundtables mit über 25 Jahren Erfahrung in der Exploit-Entwicklung erklärte, dass schnellere Updates und komplexe Ökosysteme die Zeitpläne für die Entwicklung maßgeschneiderter Tools verkürzt hätten – beispielsweise erfordert ein einziges Update der Apple-Plattform oft die Aktualisierung ganzer Ökosysteme für die Entwicklung offensiver Exploits.[20] Die Teilnehmer merkten an, dass Entwicklungen im Bereich der künstlichen Intelligenz eine kostengünstigere Entwicklung von Exploits ermöglichen könnten, dass es in diesem Bereich jedoch bisher keine öffentlichen Fortschritte gegeben habe.[21]

Allerdings erweitert sich auch der Cyberspace als Terrain: Ein neuer Operationsraum ist entstanden Es eröffnen sich Bereiche, in denen Geschwindigkeit, Skalierbarkeit und Austauschbarkeit wichtiger sind als einzelne technische Eleganz. Da Systeme immer komplexer werden und immer schneller aktualisiert werden, steigt auch die Zahl der flüchtigen Zugriffsmöglichkeiten (von komplexen „seltsamen Maschinen“ bis hin zu einfachen, falsch konfigurierten AWS-Buckets[22]).

Mit anderen Worten: **Ein Großteil der realen Cyber-Operationen erfordert keine neuartigen Zero-Day-Angriffe:** Mehrere Teilnehmer an Diskussionsrunden aus verschiedenen Branchen bestätigten, dass Credential Stuffing oder Techniken, die auf menschliches Versagen oder Lieferketten abzielen, oft ähnliche Ergebnisse mit minimalen Kosten erzielen können.[23] Das liegt vor allem daran, dass Angreifer (insbesondere solche mit geringerer Erfahrung) regelmäßig Fehler machen: Angreifer auf niedrigerer Ebene vermasseln die Befehls- und Kontrollmechanismen, konfigurieren die Infrastruktur falsch oder legen versehentlich vertrauliche Protokolle offen. Organisationen, die schnell reagieren können, könnten enorme Vorteile erzielen, indem sie einfach so viele dieser Fehler wie möglich erkennen, schnell feststellen, welche Fehler auftragsrelevanten Zugriff ermöglichen können, und diese Fehler rasch ausnutzen.

Auch die öffentliche Anerkennung des strategischen Werts kostengünstiger und schneller Ansätze wächst. Das US-Kriegsministerium (DOW) hat erkannt, dass nicht alle seine Fähigkeiten High-End-Zero-Day-Angriffe sein müssen, und ist entschlossen, mehr „Low-Equity-Fähigkeiten“ zu erwerben: Das US Cyber Command (CYBERCOM) hat für das Haushaltsjahr 2026 zusätzliche „Low-Equity-Cyber-Tools“ eingeplant, um den spezifischen Bedarf seiner Joint Task Force Zero an schneller Zugriffsgenerierung zu decken (obwohl dies nur einen kleinen Teil des Gesamtbudgets ausmacht).[24]

Während man jedoch strategisch weniger eigenkapitalintensive Kompetenzen von oben nach unten verteilen und erwerben kann, werden viele kurzlebige Zugänge im privaten Sektor von unten nach oben umgesetzt. Der private Sektor kann viele kurzlebige, opportunistische Zugänge nutzen, weil 1)

Sie verfügen über hervorragende Einblicke in Kunden- und Open-Source-Umgebungen, 2) erhalten Warnungen vor Anomalien in diesen Umgebungen und 3) verfügen über Bottom-up-Prozesse, die es einem Unternehmen ermöglichen, aufgrund dieser Einblicke schnell zu handeln. So veröffentlichte beispielsweise das defensive Cybersicherheitsunternehmen Huntress im September 2025 Informationen über die Taktik eines E-Crime-Akteurs, nachdem dieser die kostenlose Testversion von Huntress heruntergeladen und genügend verdächtige Aktivitäten durchgeführt hatte, um Signale in der EDR-Software von Huntress auszulösen.25 Dies war wahrscheinlich nur möglich, weil einzelne Analysten auf die Möglichkeit aufmerksam gemacht wurden, diese dem Management meldeten, einen Plan zur Beobachtung und Berichterstattung des Bedrohungsakteurs erstellten und die entsprechenden Genehmigungen erhielten – und das alles innerhalb kurzer Zeit.26

Im Gegensatz dazu stimmten mehrere Teilnehmer des Runden Tisches darin überein, dass die US-Regierung, ohne Der private Sektor kann nicht mit der erforderlichen Geschwindigkeit agieren, um von unten nach oben opportunistische Erfolge in dem zur Erreichung der Missionsziele erforderlichen Umfang zu erzielen.27 Das liegt wahrscheinlich daran, dass die Regierung 1) erst spät von der Chance erfährt, 2) die Nutzung der Chance nur langsam genehmigt (insbesondere aufgrund rechtlicher und politischer Beschränkungen) oder 3) nur langsam intern handelt oder die Tätigkeit auslagert. Ein Teilnehmer einer Gesprächsrunde zum Thema Regierungsaufträge fügte hinzu, dass das sich schnell verändernde digitale Ökosystem ein Problem für die Entwicklung staatlicher Betriebskonzepte (CONOP – Plan, was erreicht werden soll und wie) darstellen kann: Unabhängig von den Werkzeugen kann die Anpassung an ein neues CONOP innerhalb einer großen, bürokratischen Organisation (als Reaktion auf das sich verändernde Umfeld) langsam und operativ kostspielig sein, da die Personen, die das CONOP entwickeln, das Ziel möglicherweise nicht gut genug verstehen, um einen neuen Weg zu finden.28

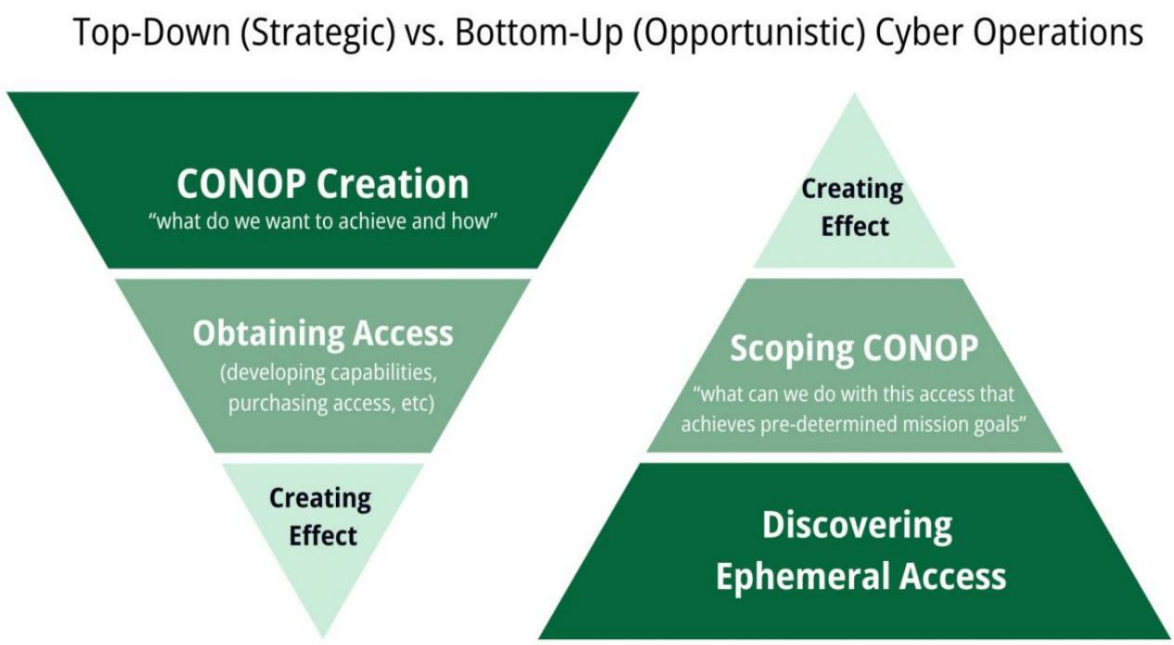


Abbildung 2: Top-Down (strategische) vs. Bottom-Up (opportunistische) Cyber-Effekte
Quelle: Winnona DeSombre Bernsen & Sergey Bratus

B. Der Privatsektor unterstützt und führt bereits Cyber-Operationen im Auftrag der US-Regierung durch

Offensive Cyber ist ein weit gefasster Begriff mit vielfältigen Bedeutungen. In diesem Zusammenhang wird offensive Cyber als Unterstützung und Durchführung offensiver Cyberoperationen (OCO) definiert. Dies umfasst die Schaffung von anfänglichen Zugriffsmöglichkeiten, Werkzeugen, Infrastruktur, Datenmanagement und Pipelines sowie die Bereitstellung von Zugriff und Effekten für OCO gemäß Titel 10 (Militär), Computernetzwerk-Exploitation (CNE)-Operationen gemäß Titel 50 (Geheimdienst) oder andere Strafverfolgungsoperationen.

Machen Sie sich nichts vor: US-Unternehmen des privaten Sektors unterstützen und führen bereits aktiv Cyber-Operationen im Auftrag der US-Regierung. Die Unternehmen tun dies auf drei Arten: Sie unterstützen **die Fähigkeiten** (d. h. sie stellen Werkzeuge, Schulungen und Infrastruktur für Cyber-Operationen bereit), verschaffen **Zugang** (d. h. sie brechen in ein System ein und geben den Zugang weiter, um weitere Regierungsmaßnahmen zu unterstützen) und erzeugen selbst **Wirkung .** Alle diese Methoden umfassen derzeit staatliche Auftragsvergabeverfahren, die Anwerbung einzelner Hacker oder Ad-hoc-Aktivitäten von Privatpersonen.

Ein Vorbehalt: Der private Sektor erzeugt bereits „Effekte“ im Cyberspace, ohne Offensive Cyber

Es ist wichtig zu beachten, dass der Großteil des privaten Sektors ohne offensive Cyberangriffe Auswirkungen auf den Cyberspace hat (d. h. Gegner stört).

Einige Auswirkungen können rein innerhalb der eigenen Infrastruktur erfolgen. Im privaten Sektor kommt es häufig vor, dass Aktivitäten auf Infrastruktur, die bereits von diesem Unternehmen bereitgestellt und gewartet wird, gestört werden (z. B. durch die Schließung von Konten, die illegale Hacking-Aktivitäten durchführen29 oder die Bereitstellung von Patches für von Angreifern ausgenutzte Software30) : Google, Microsoft, Apple, Oracle und andere große Technologieunternehmen tun dies bereits, entweder über ihre Trust-and-Safety-Teams, Abuse-Teams oder Cybersicherheitsteams. Auch die öffentliche und private Weitergabe von Indikatoren für Kompromittierungen und anderen Signaturen ist üblich. So können Unternehmen nachvollziehen, welche Bedrohungen andere Forscher beobachten, und weitere missbräuchliche Aktivitäten auf ihrer Infrastruktur unterbinden. Indikatoren werden (wenn auch über mehrere interne Rechtsberater) in der Regel an die US-Regierung weitergegeben, entweder proaktiv oder auf Anfrage der Strafverfolgungsbehörden gemäß dem Stored Communications Act31.

Weitere Effekte werden vom privaten Sektor außerhalb seiner eigenen Infrastruktur erzielt, beispielsweise über internationale Gerichtssysteme und/oder in Partnerschaft mit Strafverfolgungsbehörden. Hier liefert der private Sektor den Strafverfolgungsbehörden zusätzliche Informationen während bestehender Takedowns32

oder Beschlagnahmungen33 oder können sogar die Genehmigung eines Gerichts (über eine Zivilklage) einholen, um parallel zur Strafverfolgung Infrastrukturen, auf denen cyberkriminelle Aktivitäten stattfinden, zu beschlagnahmen oder das Eigentum daran zu übertragen. Microsofts Aktivitäten während der Abschaltung des Lumma-Stealers durch das US-Justizministerium im Mai 2025 sind nur eines von vielen Beispielen: Das US-Justizministerium erwirkte einen Haftbefehl und koordinierte die Zusammenarbeit mit Europol und dem japanischen Cybercrime Control Center, um Websites zu beschlagnahmen, die von Cyberkriminellen zur Verbreitung von LummaC2, einer Schadsoftware zum Diebstahl von Informationen, genutzt wurden. Parallel dazu leitete Microsoft eine Zivilklage ein, um 2.300 Domains, die ebenfalls von den Akteuren hinter LummaC2 genutzt wurden, zu sperren.34

Es ist wichtig zu unterscheiden, dass zivilrechtliche Beschlagnahmungen nicht durch das Eindringen in die Infrastruktur des Gegners erfolgen: Im Gerichtsbeschluss zum Fall LummaC2 wies das US-Gericht Drittparteien-Internetregister, Registrare, Rechenzentren und Hosting-Anbieter mit Niederlassungen in den USA effektiv an, in angemessener Weise dabei zu helfen, entweder die LummaC2-Domänen zu schließen oder ihr Eigentum an Microsoft zu übertragen.35 Diese zivilrechtlichen Maßnahmen sind jedoch angesichts des Zeitrahmens, der für die Erlangung eines Gerichtsbeschlusses benötigt wird, weitgehend ineffizient: Der Gerichtsbeschluss im Fall LummaC2 wurde zwei Tage nach Einreichung erlassen, und nach Entdeckung der bösartigen Domäne dauerte es wahrscheinlich noch mehrere Tage, bis er eingereicht wurde36.
Während 4–5 Tage für die Bürokratie schnell sind, ist bekannt, dass viele APT-Gruppen bösartige Domänen in weit weniger als einer Woche durchlaufen, wobei einige Domänen weniger als einen Tag aktiv bleiben.37 Darüber hinaus ist diese Taktik für die wesentlichen Teile der gegnerischen Infrastruktur, die außerhalb der Reichweite eines US-Gerichts liegen, nicht effektiv.38

US-Technologieunternehmen möchten, dass Cyber-Operationen generell von disruptiven Aktivitäten des privaten Sektors ausgeschlossen werden, da sie nicht möchten, dass Einzelpersonen Schwachstellen in ihren Plattformen ausnutzen. US-Technologieunternehmen profitieren derzeit stark von einem globalen System, in dem sie die Datenaggregation, -weiterleitung und -speicherung dominieren. Der private US-Sektor ist nach wie vor führend in den Bereichen Cloud-Infrastruktur und soziale Medien und kontrolliert somit den Großteil der weltweiten Daten. Jeder vierte Weltbürger nutzt durchschnittlich monatlich Google oder Meta, während US-Cloud-Infrastrukturdienste (AWS, Microsoft Azure, Google Cloud, Oracle, Salesforce und IBM) 70 % des Weltmarkts ausmachen.3940 Ein Großteil dieses Marktanteils (und somit der US-Wirtschaft) ist gefährdet, wenn es den Unternehmen nicht mehr gelingt, ihre Verbraucher von der Sicherheit ihrer Produkte zu überzeugen. Genau aus diesem Grund werden große Technologieunternehmen wahrscheinlich keine Mechanismen unterstützen, die offensive Aktionen des privaten Sektors ausdrücklich fördern, insbesondere solche, die Schwachstellen in ihren Plattformen ausnutzen, um in die Zielrechner einzudringen.

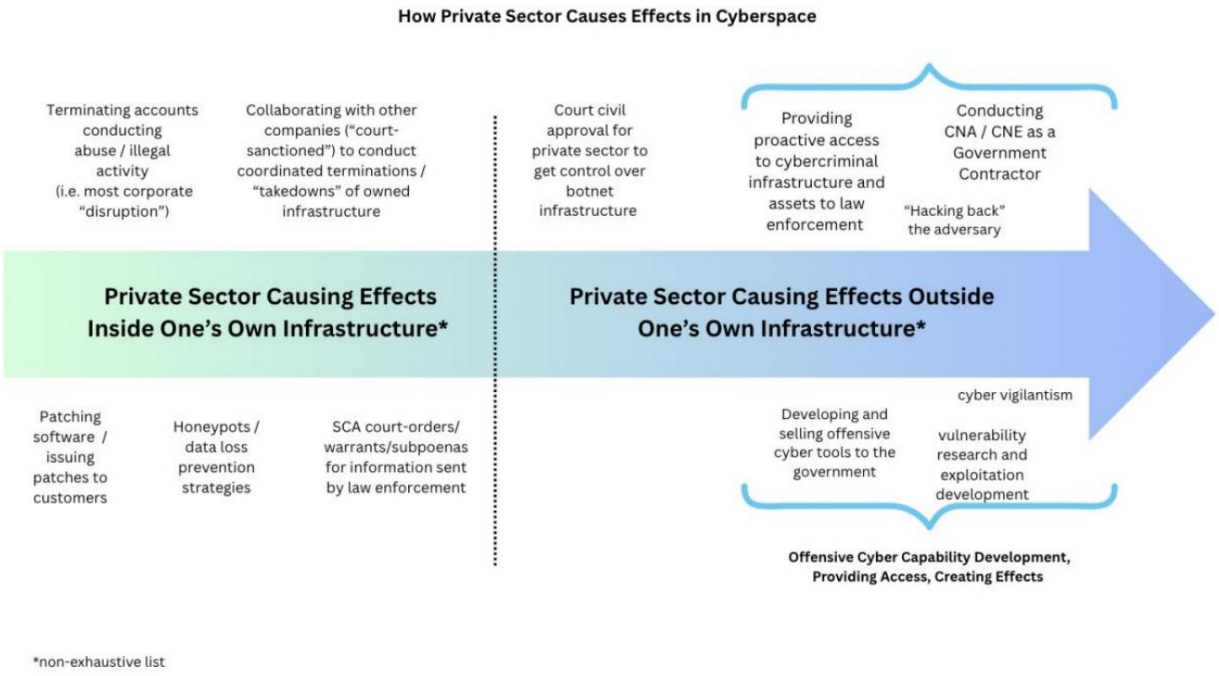


Abbildung 1: Wie der Privatsektor im Cyberspace Auswirkungen hat
Quelle: Winnona DeSombre Bernsen & Sergey Bratus

Leistungsunterstützung/Werkzeuge:

Akteure des privaten Sektors in den USA sind bereits stark in die Bereitstellung von Werkzeugen und Kapazitäten für derartige Operationen involviert: Forscher entdecken und verkaufen Schwachstellen, Implantate (also „Spyware" oder „Malware") und die dazugehörige Infrastruktur an inländische Strafverfolgungsbehörden41, ausländische Geheimdienste und Militärorganisationen42; Makler und Zwischenhändler legen Preise fest und kontrollieren Lieferketten; und Rüstungsunternehmen und Boutique-Firmen entwickeln und warten Werkzeuge für staatliche Kunden.43

Die US-Regierung (Geheimdienste, Militär und Strafverfolgungsbehörden) kauft Cyber-Kapazitäten. Einige dieser Regierungsaufträge führen zur Entwicklung einzelner Tools oder Exploits oder sogar von der Regierung genutzter Blackbox-Funktionen: Produkte, bei denen es sich um durchgängige Softwarepakete handelt, die dem Benutzer der Software Fernzugriff auf einen Zielcomputer ermöglichen.44 Hier hat die Regierung die Kontrolle über das CONOP und den eigentlichen Betrieb, allerdings mit unterschiedlichem technischen Detaillierungsgrad, da die verfügbaren Tools das technisch Machbare einschränken und Blackbox-Lösungen möglicherweise nicht genau zeigen, wie in das Ziel eingebrochen wird. Viele dieser Vertragsinstrumente sind Dienstleistungsverträge (und nicht der direkte Produkterwerb), bei denen die Unternehmen technische Ressourcen zur Verfügung stellen, um eine maßgeschneiderte Plattform oder ein Softwarepaket für die Regierung zu entwickeln und zu verwalten.

Dies wird durch die Berichterstattung zum CYBERCOM-Budget untermauert: Das Budget von CYBERCOM für Cyber Weapon Payloads (CWP) belief sich zwischen dem 1. Oktober 2024 und dem 30. September 2025 auf 160,75 Millionen Dollar, für das Haushaltsjahr 2026 sind 98,6 Millionen Dollar veranschlagt.45 Das CYBERCOM-Budget enthält zahlreiche Dienstleistungsverträge, in deren Einzelposten die Notwendigkeit einer kontinuierlichen Verbesserung der „hervorragenden Cyber-Fähigkeiten, die von internen und externen Agenturen entwickelt werden“46 genannt wird. Die Cyber National Mission Force (CNMF) von CYBERCOM, die Organisation, die mit der Verteidigung der Nation im Cyberspace durch umfassende Operationen beauftragt ist, erwirbt gezielt Fähigkeiten aus „einem vielfältigen Spektrum von Quellen, um technische Lösungen, Dienste und Werkzeuge beizusteuern“.47

Zugriff bereitstellen:

Akteure aus dem privaten Sektor bieten auch direkten Zugriff (d. h. sie brechen in einen Zielcomputer ein) auf ermöglichen Operationen der US-Regierung.

Private Zugriffe kommen in Strafverfolgungsfällen häufig vor: vor der Abschaltung durch das FBI der Qakbot-Infrastruktur im Jahr 2022 nutzte das FBI vertrauliche menschliche Quellen, um die E-Crime-Gruppe hinter Qakbot zu infiltrieren.48 Ehemalige und aktuelle Teilnehmer eines Runden Tisches der US-Regierung bestätigten, dass das FBI Informanten rekrutiert, die direkt „mit an der Tastatur“ sitzen: d. h. Privatpersonen, die im Auftrag der Regierung arbeiten und von der Regierung angewiesen werden. Solche FBI-Informanten wären wahrscheinlich über das Autorisierungsverfahren „Andernfalls illegale Aktivitäten“, das für alle vertraulichen menschlichen Quellen gilt, befugt, für einen begrenzten Zeitraum eine kleine Anzahl von Hackeraktivitäten durchzuführen.49 Im Rahmen dieser Richtlinie trägt der Informant weiterhin das zivil- und strafrechtliche Haftungsrisiko: Das FBI selbst kann keine Immunität vor Strafverfolgung durch einen Bundes- oder Staatsanwalt versprechen oder vereinbaren, kann aber das zuständige Gericht auf Anfrage über die Unterstützung des FBI durch den Informanten informieren. Teilnehmer des Dartmouth-Roundtables meinten, die Regierung könne „Zugriff“ auf ein Zielobjekt erwerben50: Ein Beispiel für einen solchen Zugriff ist der Kauf von Cellebrite, Magnet Forensics und anderen forensischen Tools durch Strafverfolgungsbehörden: Während das Produkt bestimmte Android-Zero-Days zum Entsperren von Telefonen verwenden kann, erwerben die Strafverfolgungsbehörden „Zugriff“ auf die Telefone über das forensische Tool und nicht die Zero-Day-Funktion selbst.51

In solchen Fällen verschafft ein Unternehmen der Regierung Zugang, indem es in ihrem Auftrag in einen Rechner eindringt oder der Regierung ein entsprechendes Werkzeug zur Verfügung stellt. Der Auslöser bleibt jedoch immer noch die Regierung52, die entscheidet, welche Wirkung auf den Zielrechner erzielt werden soll (d. h., ob der Zugang für Spionagezwecke oder zur Erzielung sonstiger Effekte genutzt wird). Indem der Privatsektor den Zugang gewährt, erweitert er die Optionen der Regierung. Ob diese Wahlmöglichkeit jedoch zu zusätzlichem Druck führt, ist ungewiss: Nur weil ein Akteur aus dem Privatsektor der Regierung Zugang verschafft, heißt das nicht, dass die Regierung diesen Zugang auch nutzt oder Maßnahmen ergreift, bevor der Zugang nicht mehr möglich ist.

Privatpersonen können auch proaktiv und ad hoc Zugriff gewähren, ohne eine formelle Beziehung zur US-Regierung zu haben. Hacktivisten sind beispielsweise ohne Aufforderung der Regierung in die Computer von Kriminellen eingedrungen, um Beweise für die US-Strafverfolgungsbehörden zu beschaffen.53 Im Jahr 2000 lieferte ein türkischer Hacker namens UnknownUser dem FBI proaktiv Informationen über einen Kinderpornografen, die er durch das Hacken des Computers der Person beschafft hatte.54 Auf diese begrenzte Weise können private Hacker der US-Regierung opportunistische Zugriffe verschaffen, solange sie weiterhin ohne staatliche Anweisungen oder Aufsicht agieren. Ebenso kann die US-Regierung seltene Einblicke in den privaten Sektor nutzen, die ihr sonst möglicherweise verwehrt geblieben wären.

Effekte erstellen:

Unter bestimmten Umständen werden Regierungsauftragnehmer speziell von der Regierung beauftragt um Effekte im Cyberspace zu erzielen. Die Teilnehmer der Diskussionsrunde erklärten, dass staatliche Dienstleistungsverträge im offensiven Cyberspace eine direkte Personalaufstockung beinhalten können, wobei Rüstungsunternehmen am selben Standort wie Regierungsbeamte sitzen und Cyberoperationen mit unterschiedlichem Aufsichtsgrad durchführen.55 In diesem Sinne besetzen die Rüstungsunternehmen Operationen direkt mit Personal, führen Operationen im Auftrag der US-Regierung durch und verfügen dabei rechtlich über die Autorität der Behörde.

Viele Regierungsauftragnehmer sind bereits offen für die Erbringung von Dienstleistungen für offensive Cyberoperationen, obwohl die meisten zögern, anzugeben, ob sie die Operationen selbst aktiv durchführen. Nightwing56 ist beispielsweise ein Rüstungsunternehmen mit 2.200 Mitarbeitern57 , das „Personal, Produkte und Prozesse“ für offensive Cyberoperationen bereitstellt und mit seiner Fähigkeit wirbt, „physische und virtuelle Operationen in feindlichen Umgebungen aufrechtzuerhalten“.58 Auch das CYBERCOM-Budget bestätigt die Existenz von Personalaufstockung und Fachwissen.
Der CNMF wurden im Jahr 2025 52 Millionen Dollar für die Beschaffung, Bereitstellung und Verbesserung von „Expertenvertragsdiensten“ für die Joint Task Force ZERO zur Verfügung gestellt. ZERO ist die Organisation, die für die CNMF mit der „schnellen Generierung von Zugriff“ auf Zielgeräte beauftragt ist.59 Da die Auftragnehmer als zusätzliches Personal in die Regierungsoperationen eingebunden sind, ist es sehr wahrscheinlich, dass die Regierung das CONOP und die Gesamtleitung der Operation noch immer von oben nach unten erstellt.

Unabhängig davon haben einige Akteure des privaten Sektors bereits Maßnahmen gegen Bedrohungsakteure ergriffen im Cyberspace, ohne die Regierung zu benachrichtigen oder ihr ausreichend Gelegenheit zu geben, Anweisungen zu geben. Dies führte zu unterschiedlichen Reaktionen der US-Regierung. Hack- und Leak-Operationen wurden wahrscheinlich von Privatpersonen60 durchgeführt, ohne dass die US-Regierung auf Widerstand stieß. Kampagnen von Forschern, Cyberbetrüger mit verschiedenen legalen und illegalen Mitteln zu „scambatieren“, führten ebenfalls nicht zu öffentlichen Verhaftungen von Forschern.61 Als jedoch ein US-Sicherheitsforscher im Jahr 2022 das nordkoreanische Internet für einige Tage lahmlegte (als Reaktion auf Angriffe nordkoreanischer Hacker auf ihn persönlich62), befand das FBI den Forscher für verantwortlich und rügte ihn dafür.63

C. Die US-Regierung führt Cyber-Operationen über Geheimdienste, Militär, und Strafverfolgung mit Unterstützung des privaten Sektors

Die US-Regierung ist ebenso wie der Privatsektor kein einzelner Monolith – Geheimdienste, Militär und Strafverfolgungsbehörden nutzen den Privatsektor, um im Cyberspace eine Vielzahl von Zielen zu erreichen.

Intelligenz

Die amerikanische Öffentlichkeit (und in gewissem Sinne auch der Rest der Welt) erfuhr zum ersten Mal von den USA Cyber-Operationen durch Lecks in US-Geheimdienstaktivitäten. Stuxnet im Jahr 2010 und die Snowden-Leaks im Jahr 2013 (die zu den ersten Erwähnungen der Tailored Access Operations Unit der NSA gehörten)64 waren einige der ersten Hinweise darauf, dass die US-Regierung Operationen im Cyberspace durchführte. Die US-Geheimdienste sammeln Informationen über ausländische Bedrohungen für die Vereinigten Staaten und erwerben zu diesem Zweck eine breite Palette von Software65 und Angriffskapazitäten66 vom privaten Sektor.

Um Informationen über den Cyberspace zu sammeln, müssen Geheimdienstmitarbeiter Zugriff auf das Gerät eines Ziels erhalten und dabei unentdeckt bleiben. Die US-Geheimdienste sind darin hervorragend: Durchgesickerte Dokumente67 und offene Branchengespräche68 zeigen, dass die USA hochentwickelte, langfristige Geheimdienstoperationen durchgeführt haben. Mehrere Teilnehmer des Runden Tisches aus der ehemaligen und aktuellen Regierung sowie aus der Industrie behaupteten, dass diese auf Geheimdienstinformationen fokussierte Mission der US-Cyber-Entscheidungsträger Teile der Geheimdienste davon abhalten könnte, ihre Cyber-Operationen öffentlich zu machen.69 Geheimdienstmitarbeiter sind kulturell stolz darauf, verdeckt und unentdeckt zu bleiben: so sehr, dass die NSA vor den Snowden-Leaks als „No Such Agency“ bekannt war.70 Diese Kultur dürfte sich jedoch im Laufe der Zeit ändern: Die Geheimdienste haben im letzten Jahrzehnt offener und enger mit Partnern aus dem privaten Sektor zusammengearbeitet (insbesondere mit der NSA, deren Aufgabe sowohl die Bereitstellung von Signalaufklärung als auch die Ermöglichung von Computernetzwerkoperationen umfasst, um der Nation einen entscheidenden Vorteil zu verschaffen).71

Wenn sich die Geheimdienste für einen Cyberangriff entscheiden, tun sie dies in Fällen, die als langfristig geostrategisch wertvoll gelten. Stuxnet, die mutmaßliche Cyberoperation der USA und Israels zur Sabotage iranischer Atomzentrifugen, ist ein solches Beispiel.72 Dies ist beabsichtigt: Die Befugnisse der Geheimdienste zu verdeckten Aktionen (kodifiziert in Titel 50 USC § 3093 und umgesetzt aufgrund präsidialer Verfügungen) regeln Geheimdienstoperationen, die die Verhältnisse im Ausland beeinflussen sollen, ohne dass die USA ihre Aktivitäten abstreiten können. Verdeckte Kanäle ermöglichen zwar heimliche Cyberangriffe, sind aber strukturell nicht mit der Zusammenarbeit mit dem privaten Sektor vereinbar, da gesetzliche Geheimhaltungspflichten Marktsignale, Haftungsrahmen und andere für eine nachhaltige private Beteiligung notwendige Transparenz verhindern.

Die Geheimdienste sind wahrscheinlich nicht gewillt, im Cyberspace Wirkung zu erzielen, wenn durch die Durchführung dieser Operation Zugriffe gefährdet werden könnten, die sie für die Informationsbeschaffung nutzen könnten.73 Bei jeder Geheimdienstoperation erfordert die Störung gegnerischer Systeme eine Kosten-Nutzen-Abwägung zwischen Informationsgewinn und -verlust. Dies gilt insbesondere dann, wenn die für den Zugriff erforderliche Fähigkeit teuer war und der Zugriff während der Durchführung des Effekts „verbrannt“ (d. h. entdeckt) werden könnte.74 Vereinfacht ausgedrückt: Wenn die US-Regierung eine teure Fähigkeit für die Durchführung einer Cyberoperation erwirbt – etwa eine Exploit-Kette im Wert von zehn Millionen Dollar –, kann die Nutzung dieser Exploit-Kette zur Erzielung eines Effekts weniger attraktiv sein als die Nutzung derselben Fähigkeit zur Sammlung von Geheimdienstinformationen im Wert von einem Jahr.75

Militär

Auf militärischer Seite besteht die Mission von CYBERCOM darin, Operationen durchzuführen, die Wirkung zeigen können.76 Obwohl CYBERCOM an der Bereitstellung von Cyberunterstützung für traditionelle, kinetische militärische Aktivitäten (wie die US-Angriffe auf iranische Atomanlagen im Rahmen der Operation Midnight Hammer77) oder an der Durchführung von Operationen als Reaktion auf nicht-cyberbasierte Aktivitäten beteiligt war, wurden nur wenige Details veröffentlicht. Das letzte öffentliche Beispiel war die Operation Glowing Symphony vor fast acht Jahren – als CYBERCOM zwischen 2016 und 2018 die Online-Medienaktivitäten des IS lahmlegte und es dem IS erschwerte, im Internet zu operieren.78 Stattdessen handelt es sich bei den meisten öffentlichen Operationen, die CYBERCOM zugeschrieben werden, um „Hunt Forward Operations“ – defensive Cyberoperationen, die darauf abzielen, auf Ersuchen der Partnerregierungen böswillige Aktivitäten in deren Netzwerken aufzudecken.79

Während der Kommandant von CYBERCOM durch seine Doppelfunktion sowohl die Befugnisse nach Titel 10 (Militär) als auch nach Titel 50 (Geheimdienst) innehat, unterscheiden sich die bei Cyberoperationen von CYBERCOM verwendeten Plattformen und Werkzeuge von denen der Geheimdienste.80 Dies hat nicht nur rechtliche Gründe, sondern auch, weil die Kapazitäten von unterschiedlichen Vertragsorganisationen (d. h. Unternehmen des privaten Sektors) vergeben werden und man versucht, Überschneidungen bei den Kapazitäten zu vermeiden.81 Jede „Debatte um Titel 10 vs. Titel 50“82 ist wichtig, um sowohl die rechtlichen Befugnisse zu bestimmen (d. h. wer innerhalb des Kriegsministeriums die Operation durchführt und ob der Zweck der Informationsbeschaffung oder militärischer Zwecke ist) als auch um die verwendeten Werkzeuge und Plattformen vorzuschreiben.

Leider sind die Title 10-Fähigkeiten und operativen Fähigkeiten von CYBERCOM möglicherweise weniger entwickelter als die ihrer Pendants unter Titel 50. Die „Joint Cyber Warfighting Architecture“ (JCWA)-Plattform von CYBERCOM leidet unter Interoperabilitäts- und Benutzerfreundlichkeitsproblemen, von denen einige noch behoben werden.83 Ein Teilnehmer des Runden Tisches aus dem Militär schlug vor, dass das DOW, wenn es die Wahl zwischen zwei Plattformen hätte, leicht die weiter entwickelte Plattform bevorzugen würde (wahrscheinlich eine, die für Geheimdienstoperationen verwendet wird, statt der militärischen Plattform, die für militärische Effekte konzipiert ist), was von Anfang an die Planung seines CONOP bestimmen könnte.84

Darüber hinaus deuten zahlreiche85 öffentliche Berichte über den Mangel an qualifiziertem Personal bei CYBERCOM86 darauf hin, dass es Probleme mit der Fähigkeit von CYBERCOM gibt, „Personen bereitzustellen, auszubilden und auszurüsten“. Anders ausgedrückt: Es gibt nicht genügend Uniformierte, um die Anforderungen von CYBERCOM zu erfüllen (Personen), es gibt nicht genügend wirksame Werkzeuge, um in für die Mission kritische Systeme einzudringen (Ausrüstung) und das derzeitige Personal ist nicht durchgehend gut genug im Umgang mit den aktuellen Werkzeugen geschult, um die Mission zu erfüllen (Ausbildung). Dies hat zu Forderungen nach einer „Cyber-Truppe“ geführt, um formal einen Kader militärischer Cyber-Operatoren zu schaffen.

Dies ist eine besonders interessante Dynamik für den privaten Sektor, da das US-Militär erhielt kürzlich eine Budgeterhöhung um eine Milliarde Dollar für seine offensiven Cyberoperationen, die in neue Akquisitionen von Unternehmen des privaten Sektors einfließen könnte. Der Mangel an internem Personal und unterentwickelte Plattformen lassen jedoch darauf schließen, dass Produkte und Dienstleistungen, die der private Sektor für diesen Zweig der US-Regierung herstellt, nur begrenzte Wirkung haben werden. Tatsächlich könnte ein Mangel an qualifizierten Beschaffungsbeauftragten des USCYBERCOM wahrscheinlich zur Anschaffung teurerer Produkte führen, die jedoch nicht zum Auftrag passen.

Strafverfolgung

Das FBI und der US Secret Service haben eine doppelte Verantwortung in den Bereichen Strafverfolgung und Geheimdienst. Das FBI hat offensive Cyber-Kapazitäten des privaten Sektors sowohl gekauft als auch genutzt,87 um Ermittlungen voranzutreiben: Das FBI erwarb von einem privaten Unternehmen einen Exploit, um das iPhone des Massenmörders von San Bernardino zu entsperren, und lud das kommerzielle Spyware-Unternehmen FlexiSpy vor, um gegen El Chapo, einen berüchtigten mexikanischen Drogenbaron, zu ermitteln und ihn anschließend zu verhaften.88 Das FBI kauft außerdem praktische Forensik-Tools wie Magnet Forensics89 und Cellebrite90, die Zugriff auf gesperrte Telefone ermöglichen.

Wenn die USA öffentliche Wirkung im Cyberspace erzielen wollten, geschah dies größtenteils über die Maßnahmen der Bundespolizei – obwohl die meisten dieser Maßnahmen wahrscheinlich nicht über „offensive Cyberangriffe“ erfolgten. Das Justizministerium klagt Personen an und verhaftet sie, die Computerkriminalität gegen US-Ziele begehen (dazu gehören sowohl E-Crime-Gruppen91 als auch Mitglieder ausländischer Geheimdienste92). Es beschlagnahmt auch schädliche Infrastruktur und gestohlene Vermögenswerte: Das Justizministerium hat Kryptowährungen beschlagnahmt, indem es Beschlagnahmebefehle an Kryptowährungsplattformen von Drittanbietern zugestellt hat.

Es ist möglich, dass für die Beschlagnahmung von Kryptowährungen teilweise ein Einbruch in die Maschinen ausländischer Krimineller erforderlich ist. Während einige Beschlagnahmungen von Kryptowährungen (inländische oder ausländische) durch die Zustellung von Haftbefehlen auf einer Kryptowährungsplattform möglich sind,93 erfordern andere Beschlagnahmungen von „ungehosteten“ Wallets den Besitz des privaten Schlüssels oder der Seed-Phrase eines ausländischen Kriminellen.94 Einzelpersonen schreiben ihre Seed-Phrasen normalerweise auf Papier oder speichern eine digitale Kopie (auf ihrem Laptop oder in der Cloud). Im Oktober 2025 beschlagnahmte das FBI in Zusammenarbeit mit dem US-Finanzministerium und der britischen Regierung

nicht gehostete Wallets mit 15 Milliarden US-Dollar, die einem in Kambodscha ansässigen Online-Investmentbetrugsimperium gehören – dies ist der größte von den Strafverfolgungsbehörden beschlagnahmte Einzelbetrag an Kryptowährung. 959697 Laut Anklageschrift verwaltete Chen persönlich alle privaten Schlüssel und Seed-Phrasen für seine nicht gehosteten Wallets.98 Um in den Besitz dieser Seed-Phrasen zu gelangen, hätten die Strafverfolgungsbehörden entweder 1) einen Informanten mit physischem Zugang benötigt, um an den privaten Schlüssel oder die Seed-Phrase des Kriminellen zu gelangen; oder 2) eine Person (entweder in der Regierung oder ein Informant), die in der Lage wäre, in den Laptop oder das Cloud-Laufwerk des Kriminellen einzudringen, um an die Schlüssel zu gelangen. Obwohl es keine Details darüber gibt, wie die privaten Schlüssel erlangt wurden, ist es daher möglich, dass die größte Beschlagnahmung von Kryptowährungen in der Geschichte durch Hacking erfolgte, obwohl eine physische Beschlagnahmung ebenso gut möglich ist.

Es werden Beschlagnahmungen99 und Durchsuchungen100 der mit dem Inland verbundenen Infrastruktur durch die Strafverfolgungsbehörden durchgeführt mit einem ähnlichen Verfahren wie bei der Beschlagnahmung von Kryptowährungen im Inland – der Zustellung von Haftbefehlen an Drittplattformen. Wenn die Infrastruktur nicht im Besitz eines US-Unternehmens ist oder sich physisch in den USA befindet Die Ermittlungen werden jedoch häufig über informelle Anfragen oder über Rechtshilfeabkommen (Mutual Legal Assistance Treaties, MLAT) abgewickelt: ein notorisch langsamer und mühsamer Prozess zwischen US-amerikanischen und internationalen Strafverfolgungsbehörden.101 Wenn die Partner zur Zusammenarbeit bereit sind, sind in diesem Prozess einige deutliche Erfolge zu verzeichnen: US-amerikanische Strafverfolgungsbehörden haben im Rahmen der Operation Endgame mit privaten Unternehmen und Interpol zusammengearbeitet und dabei die wichtige Infrastruktur hinter der für Ransomware-Angriffe verwendeten Schadsoftware zerschlagen.102 Das FBI arbeitete auch mit der niederländischen Polizei zusammen, um die Server von El Chapo anzuzapfen (die auf Ersuchen des FBI von einem vertraulichen Informanten aus Kanada in die Niederlande transferiert wurden).103104

D. Risikokapital investiert überwiegend in defensive statt offensive Cyber-Maßnahmen. Weil offensive Cyberangriffe traditionell forschungsintensiv und dienstleistungsorientiert sind Vertragsbasiert

Offensive Cyber-Unternehmen benötigen wie andere Firmen, die auf Regierungsaufträge angewiesen sind, vor ihrem ersten Verkauf häufig Unterstützung und private Finanzierung.105 Während sich einige Berichte auf Private-Equity-Investitionen in etablierte offensive Cyber-Unternehmen konzentrierten, wurde sehr wenig über Risikokapital und anfängliche Startkapitalinvestitionen für neue Firmen berichtet, die auf den Markt drängen.106

Trotz des gestiegenen Risikokapitalinteresses an Dual-Use- und Angriffstechnologien107 konzentriert sich das Finanzierungsinteresse im Cyberbereich nach wie vor auf defensive Cyberlösungen.108
Die Portfolios von Risikokapitalfirmen wie In-Q-Tel bevorzugen nach wie vor überwiegend kommerzielle defensive oder Dual-Use-Technologien109.

Risikokapitalgeber und Branchenteilnehmer des Dartmouth-Roundtables gaben an, dass dies wahrscheinlich daran liegt, dass kommerzielle Verteidigungstechnologien klarere Marktanwendungen und vorhersehbarere Einnahmequellen haben als ihre offensiven Gegenstücke. 110 Dies gilt insbesondere für die Verletzlichkeit

Forschung, da man nicht im Voraus wissen kann, welche Schwachstellen gefunden werden oder wie lange sie bestehen bleiben.111 Reine Dienstleistungsunternehmen sind für Risikokapitalfonds schwer zu rechtfertigen, da sie nicht gut skalierbar sind, auf eine kleine Anzahl hochwertiger Kunden angewiesen sind und ihnen die Vorhersehbarkeit wiederkehrender Einnahmen fehlt, die für die Unterstützung eines klassischen VC-Renditemodells erforderlich ist. Unternehmen hatten in der Vergangenheit auch Schwierigkeiten, offensive Geschäftsmodelle zu gründen, die ein Abonnement-Softwaremodell mit jährlich wiederkehrenden Einnahmen nachahmen, da offensive Arbeit tendenziell dienstleistungslastig wird, bei dem Kunden für Fachwissen und Zeit zahlen, nicht für eine reproduzierbare Plattform.112

Darüber hinaus haben offensive Unternehmen zusätzliche Probleme mit dem Kundenkonzentrationsrisiko, das potenzielles Wachstum und Anlegerrenditen begrenzt. Offensive Unternehmen sind oft nur auf eine Handvoll großer Regierungs- oder Hauptauftraggeber angewiesen, während defensive Unternehmen an die meisten Kunden verkaufen können, ob öffentlich oder privat, im In- oder Ausland. Diese Konzentration auf hauptsächlich US-Regierungs- und FVEY-Kunden bedeutet, dass eine einzige Änderung der Beschaffung, eine Politikänderung oder eine Freigabeentscheidung die Einnahmen über Nacht zunichtemachen kann.113 Diese Abhängigkeit von nur wenigen Regierungskunden schränkt auch die Ausstiegsmöglichkeiten ein – offensive Unternehmen werden wahrscheinlich nicht an die Börse gehen, sondern stattdessen wahrscheinlich von einem größeren Hauptauftraggeber im Verteidigungssektor oder von Private-Equity-Firmen aufgekauft werden: Boldend114, Azimuth und Kudu Dynamics115 sind allesamt kleine bis mittelgroße offensive Unternehmen, die in den letzten fünf Jahren von größeren Rüstungsunternehmen übernommen wurden. Die NSO Group, ein großes israelisches Access-as-a-Service-Unternehmen, das mit Menschenrechtsverletzungen in Verbindung gebracht wird, wurde sowohl 2014 als auch im Oktober 2025 von einer US-amerikanischen Private-Equity-Firma aufgekauft.116

Offensive Unternehmen können breitere Exit-Möglichkeiten finden, wenn sie ihr Geschäft umstellen und sich weitgehend auf defensive Anwendungsfälle konzentrieren: Endgame, einst als „Blackwater des Hackings“117 bezeichnet, holte 2012 CEO Nathaniel Fick an Bord, um die kommerziellen und staatlichen Angebote des Unternehmens auszubauen118 und wurde 2019 von Elastic übernommen. Zu diesem Zeitpunkt hatte sich das Unternehmen weitgehend auf die Bereitstellung von „Endpunktschutz, -erkennung und -reaktion“119 konzentriert. Diese Optionalität führt jedoch nicht unbedingt zu zusätzlichen Gewinnen (Endgame wurde für 234 Millionen Dollar über Elastic-Aktien und Schuldentilgung übernommen, während Kudu in einer Barübernahme für 300 Millionen Dollar erworben wurde).120

Nebenbei bemerkt, viele Investoren freuen sich auch über sichtbare Ergebnisse: ein runder Tisch
Ein Teilnehmer bemerkte, dass die Geheimhaltung aufgrund der oft geheimen, auf Geheimdienstinformationen basierenden Verträge mit der Regierung es schwierig mache, den Investoren solche Ergebnisse vorzulegen.121

Die offensive Cyber-Industrie – Lücken und Chancen

1. **Lücke:** Die aktuellen Möglichkeiten der US-Regierung, den privaten Sektor einzubeziehen
   Offensive Cyber-Maßnahmen erzielen nicht genügend Ergebnisse, insbesondere nicht für Bottom-Up-Maßnahmen
   Gelegenheiten

Der Geheimdienst, das Militär und die Strafverfolgungsbehörden der Vereinigten Staaten sind auf vorsätzliche, eng abgegrenzte, Top-down-Operationen im Cyberspace. Dies führt jedoch nicht zu offensiven Cyber-Ergebnissen in dem von den US-Politikern geforderten Tempo. Zudem kann der Privatsektor zwar auf neue, zeitkritische Bottom-up-Möglichkeiten reagieren, die sich durch Fehler des Gegners ergeben, doch das operative Tempo der Regierung kann wahrscheinlich nicht mithalten.

Die Struktur der Geheimdienste legt Wert auf langfristige Geheimaktivitäten und ihre Kultur lehnt es ab, kurzfristige Effekte zu erzielen, insbesondere wenn dadurch die Gefahr besteht, dass teure Ressourcen verschwendet werden. Die Fähigkeit von CYBERCOM, in großem Maßstab Wirkung zu erzielen, wird durch anhaltende Probleme mit der Ausstattung und dem Personal eingeschränkt. Schließlich sind die Strafverfolgungsbehörden, vor allem das FBI und das Justizministerium (DOJ), die sichtbarsten Ausführenden der US-Cyberoperationen, werden jedoch durch ihre Mission und Befugnisse eingeschränkt. Zusammengenommen erzeugen diese institutionellen Silos ein fragmentiertes Ökosystem, das Operationen in dem für den Wettbewerb im Cyberspace erforderlichen Umfang nicht unterstützt. Wenn sich intern zeitkritische Gelegenheiten ergeben, fehlt den USA daher möglicherweise die verfahrenstechnische und rechtliche Infrastruktur oder sogar die Ressourcen, um entschlossen zu handeln.

Darüber hinaus führt die derzeitige Struktur der US-Regierung zur Nutzung privater Akteure (starre Vertragsgestaltung, Rekrutierung oder proaktive Selbstjustiz) zwar zu technischen Spitzenleistungen, ist aber kein skalierbares System für schnelle, legale und wiederholbare offensive Cyberoperationen – weder durch Top-down-Aufgaben noch durch Bottom-up-Möglichkeiten. Ein Großteil der offensiven Instrumente des Landes ist nach wie vor durch maßgeschneiderte Dienstleistungsverträge statt durch skalierbare, interoperable Plattformen gesichert. Vertrauliche Personalbeschaffungsbeziehungen sind stark individualisiert, zeitlich begrenzt und mit rechtlichen Unklarheiten behaftet. Die Auswirkungen auf den privaten Sektor werden entweder von der Regierung streng von oben nach unten überwacht oder überraschen die Regierung außerhalb staatlicher Kanäle. Dies zeigt eine klare Lücke: Es besteht ein ausgeprägter Wunsch der politischen Entscheidungsträger, unsere Cyber-Delikte auszuweiten, aber es gibt keine groß angelegten Kanäle für die US-Regierung, um mit privaten Unternehmen zusammenzuarbeiten.

2. **Chance:** Der private Sektor ist in der Lage und bereit, offensive Cyber-Fähigkeiten und -Zugang in einem größeren Umfang bereitzustellen, als derzeit genutzt wird

Glücklicherweise verfügt der private Sektor bereits über die technischen Fähigkeiten, Werkzeuge und operativen Erfahrungen, die erforderlich sind, um sowohl hervorragende als auch kostengünstige Angriffsfähigkeiten sowie einen schnellen, zeitnahen und umfassenden Zugang bereitzustellen, und ist bereit, der Regierung weitere Fähigkeiten und Zugangsmöglichkeiten zu bieten.

Fähigkeiten/ Tools

Mehrere Teilnehmer an Risikokapital- und Branchen-Roundtables waren sich einig, dass auf dem US-Markt die Chance besteht, eine Handvoll privater Unternehmen aufzubauen, die das auf Dienstleistungen und Verteidigung ausgerichtete Modell offensiver Cyber-Tools aufbrechen: weg von maßgeschneiderten Dienstleistungen hin zu etwas, das stärker auf das Produkt ausgerichtet ist, was auch ein besseres Geschäftsmodell für private Geldgeber sein kann.122

Unternehmen haben Verteidigungstechnologie bereits in anderen Bereichen als Produkt neu konzipiert. So wurde Anduril zum Liebling der Verteidigungstechnologiebranche, indem das Unternehmen eine einzige, aber wesentliche Änderung am Geschäftsmodell der Verteidigungsindustrie vornahm: Die Forschung erfolgte nicht mehr über Dienstleistungsverträge. Stattdessen investierte Anduril im Vorfeld privat in Forschung und Entwicklung und lieferte fertige Systeme, um langsame Beschaffungszyklen zu umgehen.123

Die Fähigkeit des privaten Sektors, offensive Cyber-Effekte abzuwehren, ist bereits vorhanden und Vielschichtig: Unternehmen können gleichzeitig kostengünstige, hochvolumige Funktionen (durchgesickerte Anmeldeinformationen, Protokollierung falsch konfigurierter Buckets usw.) sowie komplexe, maßgeschneiderte Zero-Day-Angriffe verfolgen, die intensivere Forschung und Entwicklung erfordern. In der Praxis schließen sich diese nicht gegenseitig aus, insbesondere wenn KI in diesem Bereich zu einem Schlüsselfaktor für Skalierung wird. Mehrere Teilnehmer der Diskussionsrunde waren sich einig, dass Automatisierung und KI wahrscheinlich auch zu zentralen Schlüsselfaktoren für diese Größenordnung werden.124 Die Industrie hat bereits begonnen, LLMs und Fuzzing in offensive F&E-Workflows und Sicherheitswettbewerbe zu integrieren.125

Diese Dualität von hoher und niedriger Eigenkapitalfähigkeit ist wichtig, weil nicht jede Mission erfordert die gleiche Treue bzw. Risikobereitschaft; was zählt, ist die Abstimmung der Fähigkeiten auf die Ziele, das Vorhandensein von „Dingen auf Lager“, die ausdrücklich für die Mission entwickelt wurden, die sie erfüllen sollen, oder die Fähigkeit, schnell ein Werkzeug zu erstellen, wenn eine Operation eine unerwartete Wendung nimmt.

Zugang

Der Privatsektor ist wahrscheinlich auch bereit, weitere Unternehmen zu gründen, die das Vertrauen genießen und die Fähigkeit, der Regierung tatsächlichen „Zugriff“ zu gewähren, indem im Auftrag der Regierung in Systeme eingebrochen wird.

Einige dieser Möglichkeiten lassen sich trivial mit den oben genannten Low-Equity-Funktionen kombinieren: Wenn

Wenn beispielsweise die Anmeldeinformationen kompromittiert wurden, lässt sich leicht erkennen, ob die Anmeldeinformationen tatsächlich funktionieren (und so unberechtigten Zugriff auf einen Zielcomputer erhalten). Erfolg im großen Maßstab erfordert ein tiefgreifendes Verständnis der Systeme und Abwehrprozesse des Gegners: In der Praxis bedeutet dies, opportunistisch auf Low-Level-Zugriffe in einer ausreichend großen Menge abzuzielen, um eine Wirkung auf die Mission zu erzielen, und gleichzeitig Pipelines aufzubauen, die die Erfassung von Daten und Fähigkeiten, sichere Tests und eine schnelle Bereitstellung integrieren.

Die Wirtschaftlichkeit wäre für neue Unternehmen äußerst attraktiv, wenn die richtigen Beschaffungs- und Anreizstrukturen geschaffen würden. So könnten kleinere Unternehmen, die offensive Cyber-Zugänge produzieren, Dienstleistungsverträge, die größtenteils nur Generalunternehmern vorbehalten sind, möglicherweise stören – und so Gewinne erzielen, Ineffizienzen bei der Beschaffung reduzieren und Kosteneinsparungen an den Staat weitergeben.126 Durch die Schaffung von Zugangsplattformen statt Dienstleistungen wären die Unternehmen zudem wahrscheinlich attraktiver für Risikokapitalinvestitionen.

Durch die Bereitstellung des Zugangs könnten auch zusätzliche, wenn auch unkonventionellere Wertpools erschlossen werden. Beispielsweise könnte die Schaffung eines Kopfgeldmodells für die Beschlagnahmung und Wiederbeschaffung von Krypto-Vermögenswerten bei entsprechender Genehmigung und Steuerung eine enorme Verdienstmöglichkeit für aufstrebende Unternehmen darstellen. Da diese Zugriffe über ein Produkt erfolgen könnten und regelmäßigere Auszahlungen möglich wären, wären Risikokapitalgeber und andere Investoren deutlich stärker an einer Investition interessiert.

Natürlich gibt es bei diesem Geschäftsmodell eine Reihe rechtlicher Risiken. Für private Unternehmen ist die Der Computer Fraud and Abuse Act (CFAA) ist das wichtigste rechtliche Hindernis für den Zugriff auf Zielgeräte, da das Gesetz den unbefugten Zugriff auf Computersysteme unter Strafe stellt. Von der Bereitstellung eines Exploits bis hin zur Ausnutzung von Cloud-Fehlkonfigurationen – alles ist gemäß dem CFAA illegales Hacking, wenn es ohne Genehmigung erfolgt.127 Das bedeutet, dass der Zugriff sowohl im Inland als auch im Ausland straf- und zivilrechtliche Haftungsrisiken birgt. Obwohl der CFAA eine Ausnahme für „rechtmäßig autorisierte Ermittlungs-, Schutz- oder Geheimdienstaktivitäten von US-amerikanischen Strafverfolgungs- oder Geheimdiensten“ vorsieht, wurde dies nie offen definiert oder vor Gericht geprüft.128

Darüber hinaus erfolgt die Autorisierung wahrscheinlich unter geheimen Umständen, was die Bedenken hinsichtlich Greymail verstärkt und Unternehmen daran hindert, offener mit Anwälten oder Investoren auf dem Markt zu sprechen.129

Viele Organisationen leben jedoch bereits mit diesem rechtlichen Risiko – wie bereits erwähnt, gewähren sowohl Einzelpersonen als auch Unternehmen der US-Regierung bereits Zugriff.
Noch mehr Firmen in der defensiven Cybersicherheitsbranche, wie etwa in der Bug-Bounty-Branche, betreiben Sicherheitsforschung auf eine Weise, die den autorisierten Zugriff überschreitet. Das Justizministerium verfolgt solche privaten Firmen wahrscheinlich nicht, weil dies derzeit „nicht den Interessen der US-Regierung dient“.130
Mehrere Teilnehmer der Diskussionsrunde merkten außerdem an, dass Geschworenengerichte eine Person oder Organisation, die einen Cyberkriminellen verfolgt, wahrscheinlich nicht verurteilen würden. Dies könnte sich jedoch ändern, wenn durch einen solchen Zugriff des privaten Sektors unbeabsichtigter Schaden entstehen würde.131

Die Teilnehmer der Gesprächsrunde merkten an, dass Bedenken hinsichtlich einer Eskalation132 und eines Reputationsrisikos sowie Sicherheitsbedenken sowohl für den staatlichen als auch für den privaten Sektor in politischen Diskussionen häufig überbewertet werden.133 Obwohl beispielsweise das Risiko von Reputationsschäden und Sicherheitsbedenken nach wie vor hoch ist, agieren viele Rüstungsunternehmen und Sicherheitsfirmen bereits in umkämpften Umgebungen und akzeptieren bestimmte operative Risiken: So greifen Nordkorea und andere staatliche Akteure bereits routinemäßig offensive Sicherheitsforscher allein wegen ihrer Tools an, und die Unternehmen haben ihre Haltung gegenüber OPSEC entsprechend geändert.134

Kurz gesagt: Sowohl die Technologie als auch das Kapital sind vorhanden. Was noch fehlt, ist die Schaffung politischer und rechtlicher Schutzmechanismen, Kontrollmechanismen, Nachfragesignale und Beschaffungsinstrumente, damit private Unternehmen glaubwürdige, investitionswürdige offensive Cyberplattformen aufbauen können, die vorhersehbare Ergebnisse für die nationale Sicherheit liefern.

3. **Chance:** Der Privatsektor ist in der Lage und willens, zusätzliche Maßnahmen gegen Ziele niedrigerer Ebene zu ergreifen, wenn er über angemessene zivilrechtliche Haftung, Aufsicht und andere Schutzmechanismen verfügt.

Auch private Akteure sind wahrscheinlich bereit, im Auftrag der US-Regierung rasche Maßnahmen gegen begrenzte, weniger risikoreiche Ziele zu ergreifen. Dafür bräuchten sie jedoch zusätzliche Haftungs- und Sicherheitsgarantien sowie Kontrollmechanismen. Würden sie solche Aktivitäten dem privaten Sektor überlassen, würden die US-Regierung Ressourcen freisetzen, die sie auf vorrangigere Ziele konzentrieren könnte.
Die Teilnehmer des Runden Tisches in Dartmouth zeigten größtenteils nur wenig Begeisterung für privatwirtschaftliche Aktivitäten, die unabhängig von direkten Regierungsaufträgen sind.135

Obwohl einige Politiker darauf beharrten, dass die Auswirkungen auf den privaten Sektor „die
Obwohl die Privatwirtschaft gegen China vorgeht, könnte sie davor zurückschrecken, Akteure ins Visier zu nehmen, die als höheres Risiko wahrgenommen werden – sei es für die Sicherheit einzelner Forscher oder aus geopolitischer Sicht im Allgemeinen.
Branchenteilnehmer stellten fest, dass das Risiko für die körperliche Unversehrtheit je nach Akteur unterschiedlich ist: Während Angriffe auf Nordkorea, mit China verbundene Akteure niedrigerer Ebene und Ransomware-Akteure wahrscheinlich keine Bedrohung für das Leben eines Forschers darstellen würden (und für Unternehmen unbedenklich wären), könnten einige Kartelle (und bestimmte andere in China ansässige Organisationen136) über die Ressourcen verfügen, um mit direkter körperlicher Gewalt Vergeltung zu üben, was ein zu großes Risiko darstellt.
137

Die Teilnehmer der Diskussionsrunde schienen jedoch von einem Programm ermutigt zu sein, mit dem private Akteure gezielt Bedrohungsakteure ins Visier nehmen können, die ein geringeres Risiko für die Sicherheit der Forscher und die Geopolitik darstellen. Die Teilnehmer der Diskussionsrunde betonten zudem die Notwendigkeit einer gewissen Aufsicht und eines optionalen Genehmigungsmechanismus, um sicherzustellen, dass sie 1) nicht in laufende Regierungsoperationen eingreifen, 2) nicht versehentlich gegen andere Bundesgesetze (wie den Wiretap Act oder den ECPA) verstoßen und 3) ihre Operationen auch ansonsten sicher und maßgeschneidert durchführen.138
Obwohl, wie im oben genannten Fall der Strafverfolgungsabordnung bezüglich FISA gezeigt, es wahrscheinlich Mechanismen gibt, durch die die Regierung diese Aufsicht gewährleisten kann. Regierungsbeteiligte

deutete an, dass diese Ziele für die US-Regierung möglicherweise von geringem Interesse seien, insbesondere angesichts der Ressourcen, die für die Überwachung privater Akteure erforderlich sein könnten.

Unabhängig von Programm oder Ziel bleibt die zivilrechtliche Haftung wahrscheinlich das stärkste Abschreckungsmittel für private Unternehmen. Die Auswirkung auf eine Maschine kann gemäß dem CFAA als „Schaden“ gelten und birgt weiteres Risiko straf- und zivilrechtlicher Haftung – insbesondere, wenn die Auswirkung unbeabsichtigte Folgen hat. Betreiber externer Infrastrukturen, Cloud-Anbieter oder ausländische Unternehmen können Unternehmen, die westliche Technologiesysteme ausnutzen, bereits problemlos verklagen.139 Viele solcher Fälle gibt es bereits in der Bug-Bounty-Branche, wo Softwareanbieter Zwangsunterlassungserklärungen gegen einzelne Bug-Hunter erlassen haben, die defensive Forschung betreiben.140 Trotz der Bemühungen des Justizministeriums, eine Richtlinie zur Nichtverfolgung von Sicherheitsforschung im guten Glauben zu schaffen, berichteten Forscher, dass die Androhung einer Klage einen abschreckenden Effekt hat, der anhält, da die Richtlinie nicht den gleichen Schutz bietet wie der volle gesetzliche Schutz. Wie mehrere anmerkten: „Es ist eine Richtlinie, kein Gesetz.“141

Die Teilnehmer des Runden Tisches waren sich nicht einig, wie viel Haftungsschutz der private Sektor bräuchte jedoch Maßnahmen – insbesondere, wenn der Privatsektor einen Fehler macht. Ein Teilnehmer brachte die Stimmung klar auf den Punkt: „Ich werde für eine meiner Firmen keinen Vertrag unterschreiben, in dem steht, dass die US-Regierung, wenn sie etwas im Zusammenhang mit der US-Regierung tut, freie Hand hat, sie zu verklagen, wenn sie das falsche Ziel trifft.“142

Damit hat die US-Regierung die Möglichkeit, eine rechtliche und/oder regulatorische Aufsichts- und Genehmigungsmodell, das es dem privaten Sektor ermöglichen würde, im Cyberspace opportunistischer gegen weniger risikobehaftete Akteure vorzugehen, während die US-Regierung gleichzeitig genügend Kontrolle über den Prozess hätte, um einen minimalen Kollateralschaden zu gewährleisten.

4. **Lücke:** Der US-Regierung fehlt die Transparenz, um einen klaren Bedarf an offensiven Cyber-

Die US-Regierung ist in der Lage, hochqualifizierte Fachkräfte anzuwerben und Verträge mit großen Generalunternehmern abzuschließen.143 Allerdings ist es ihr bisher nicht gelungen, ein ausreichend starkes Nachfragesignal im Bereich offensiver Cybersicherheit zu erzeugen, um Finanzmittel und Kapital in effektive Teams fließen zu lassen.

Derzeit gibt es keine öffentliche, programmatische Verpflichtung der US-Regierung, die Investoren und Unternehmern sagt: „Bauen Sie ein Angebot im offensiven Cyberbereich auf, und wir werden es kaufen und aufrechterhalten.“ Das Ergebnis ist, dass Kapital in defensive, produktionsfähige Technologien fließt, während offensive Arbeiten unterfinanziert und ad hoc durchgeführt werden.

Damit Investoren und Unternehmen verstärkt in den Markt einsteigen, benötigen sie klarere politische Signale, um zu wissen, was die Regierung braucht, um zu entscheiden, was finanziert oder gebaut werden soll. Ohne klare Missionsbeschreibungen und Ergebniskennzahlen fällt es selbst erfahrenen Teilnehmern schwer, zu erkennen

wie ihre Bemühungen zu den nationalen Zielen beitragen. Wenn die Strategie und die Anforderungen der Regierung undurchsichtig sind, können nur erfahrene Insider das Signal analysieren – die meisten Investoren sind keine erfahrenen Insider und werden angesichts solcher Unklarheiten kein Kapital investieren.144

Dieses schwache Nachfragesignal wird durch Komplexität und Geheimhaltung noch verstärkt. Offensive Cyber Die Arbeit erfordert zwangsläufig die Einbeziehung von Kompetenzen, Autoritäten und Behörden, und ein Großteil dieser Aktivitäten unterliegt der Geheimhaltung. Diese Geheimhaltung steht im Widerspruch zu den Anforderungen privater Investoren: Risikokapitalgeber wollen verstehen, was ein Unternehmen baut, welche politischen Probleme es anspricht und welches wiederholbare Ertragsmodell einen Ausstieg ermöglicht.145

5. **Chance:** Forschungseinrichtungen zum Verständnis von Software und offensiver Sicherheit können neue Forschungen beschleunigen, um neue Lösungen zu entwickeln

Die Weird-Machine-Theorie besagt, dass 1) die Komplexität eines angegriffenen Programms dem Angreifer zugutekommt;146 und 2) das Verständnis eines Programms zum Aufbau sicherer Systeme ein Verständnis der Ausnutzbarkeit des Systems selbst erfordert.147 Obwohl das Verständnis von Software sowohl für die nationale Sicherheit als auch für die technologische Wettbewerbsfähigkeit von zentraler Bedeutung ist, wird in akademischen und staatlichen Forschungs- und Entwicklungsprogrammen angewandter IT und defensiver Cybersicherheit immer noch Vorrang vor offensiver Forschung oder sogar Dual-Use-Analysen zum tatsächlichen Verhalten und Versagen moderner Softwaresysteme eingeräumt.148 Derzeit lehren nur wenige amerikanische Universitäten wie Dartmouth Techniken zum Verständnis von Software, die das Studium der Protokollinteraktion, des Ausführungsflusses, des Timings und der Logikfehler fördern, auf die sich die Angreifer selbst verlassen. Dies öffnet Tür und Tor für aktive Cyber-Gegenmaßnahmen: die gezielte Schaffung von Umgebungen, die feindliche Aktivitäten ohne Eskalations- oder Attributionsrisiko absorbieren, untersuchen und neutralisieren.

In einer Zeit, in der offensive Vorteile von Geschwindigkeit, Automatisierung und kreativer Improvisation abhängen, können nur Institutionen, die die Funktionsweise von Systemen verstehen (aufgrund der Theorie seltsamer Maschinen oder des Softwareverständnisses), diese emergenten Eigenschaften vorhersehen und ausnutzen, bevor es Gegner tun. Die Priorisierung dieses Bereichs an Universitäten und Forschungszentren stellt sicher, dass zukünftige Betreiber, Analysten und politische Entscheidungsträger von der Reaktion auf Eindringlinge zur Entwicklung widerstandsfähiger, adaptiver Systeme übergehen können – und dieses Verständnis gegebenenfalls nutzen können, um das Verhalten von Gegnern so zu beeinflussen, dass nationale Interessen geschützt werden. Das Verständnis umfassenderer Systeme (nicht nur der Software selbst) könnte zudem zur Entdeckung weiterer flüchtiger Zugriffe oder sogar zusätzlicher Möglichkeiten führen, die Umwelt zu beeinflussen, die überhaupt keine offensive Cybersicherheit erfordern.

Empfehlungen - Die Zukunft offensiver Cybersicherheit nutzen in der Privatsektor

Die nächste Phase offensiver Cyber-Macht wird nicht davon abhängen, den nächsten Zero-Day zu finden, sondern auf der Suche nach einem (rechtlichen, finanziellen und kulturellen) Modell, das alle Formen offensiver Cyberangriffe in großem Maßstab eindämmen kann. Daher werden auf Grundlage der wichtigsten Ergebnisse des Dartmouth-Roundtables die folgenden Empfehlungen gegeben:

1. Entwickeln Sie eine öffentliche offensive Cyber-Strategie

Insgesamt haben die USA einen strategischen Wendepunkt bei offensiven Cyberoperationen erreicht. Der aktuelle Ansatz, der auf Ad-hoc-Beziehungen, maßgeschneiderten Verträgen und undurchsichtigen Prozessen basiert, ist den Anforderungen moderner Konflikte und anhaltender Auseinandersetzungen nicht gewachsen. Das Weiße Haus muss diese Ad-hoc-Ansätze in einer einheitlichen, öffentlichen offensiven Cyberstrategie vereinen.

Seit zwei Jahrzehnten wird eine nationale offensive Cyberstrategie gefordert: Eine solche Anstrengung könnte dieses Flickwerk in ein öffentlich erklärtes, organisiertes Ökosystem verwandeln, das private Innovationen, die Zusammenarbeit mit internationalen Verbündeten und die Entwicklung staatlicher Fähigkeiten unter einer gemeinsamen Vision und einem klaren Nachfragesignal vereint.149

Durch die Formulierung einer Vision für offensive Cyberangriffe kann die Regierung die Grenzen zwischen rechtmäßigen, strategischen Operationen und rücksichtsloser Störung klarstellen und gleichzeitig die Vorgehensweise der USA von der von Gegnern wie China, Nordkorea oder Russland unterscheiden, deren offensive Ansätze des privaten Sektors häufig systemische Risiken für globale Netzwerke mit sich bringen.150 Klare strategische Ergebnisse könnten sein: verbesserte und skalierte offensive Cyber-Lieferketten der USA, eine langfristige und gestärkte Pipeline offensiver Cyber-Talente aus dem privaten Sektor, eine klare operative Aufteilung der Verantwortung zwischen Regierung und privatem Sektor im Cyberspace und eine langfristige Schwächung der Fähigkeiten des Gegners.

Eine ausgereifte Strategie muss auch die politische Vorstellungskraft hinsichtlich des Zwecks offensiver Cyberangriffe erweitern. Cyberoperationen sollten nicht ausschließlich als Gegenmaßnahmen gegen Cyberangriffe konzipiert werden. Großbritannien hat bereits eingeräumt, Cyberangriffe „für eine Reihe von außenpolitischen, militärischen und öffentlichen Zielen“ einzusetzen, nicht nur als Vergeltung für digitale Vorfälle.151 Ebenso sollte die US-Doktrin Cyberangriffe als proaktives, bereichsübergreifendes Instrument staatlicher Kunst betrachten. Dies erfordert eine bessere Abstimmung der Fähigkeiten auf die Ziele – die Erkenntnis, dass hochrangige Ziele wie Natanz Milliardeninvestitionen und verdeckte Behördenmaßnahmen verdienen, während andere Ziele schnellere und deutlichere Effekte des privaten Sektors erfordern.

Mehr Transparenz würde auch eine bessere Koordinierung, politische Abstimmung und gezieltere Ausrichtung zwischen internationalen Partnern und der Five Eyes-Allianz ermöglichen. Dies ist besonders wichtig, da

Australien investiert stärker in seine offensiven Cyberfähigkeiten152 und Großbritannien denkt über die künftige Ausrichtung seiner National Cyber Force nach. Die britische National Cyber Force hat ihre Grundsätze für eine verantwortungsvolle Cybermacht in der Praxis bewusst veröffentlicht und stellt Angriffe nicht als ein Instrument betrügerischer Machenschaften dar, sondern als ein kalibriertes Instrument staatlicher Kunst, das verantwortungsvoll, präzise und kalibriert sein soll.153 Die USA können dasselbe tun – wie ein Teilnehmer einer politischen Diskussionsrunde witzelte: „Wir müssen aufhören, so zu tun, als würden wir nichts tun.“

Dies ist kein Aufruf, die Cyber-Offensive zu verstärken und gleichzeitig die Verteidigung zu vernachlässigen – ganz im Gegenteil. Derzeit bevorzugt der US-Cybermarkt insgesamt defensive Aktivitäten154: Jede offensive Cyberstrategie muss selbstverständlich Hand in Hand mit defensiven Maßnahmen gehen. Die Entwicklung einer offensiven Cyberstrategie würde einen expliziteren Dialog mit der defensiven Community ermöglichen, darunter auch mit einigen der Unternehmen, die für die Sicherung der US-Netzwerke verantwortlich sind. Zudem würde sie klare Koordinierungsbemühungen schaffen, um sicherzustellen, dass offensive Cyberbemühungen der USA nicht die Gefahr bergen, unsere eigene nationale Sicherheit zu gefährden.

In ähnlicher Weise könnten auch die Geheimdienste und das Militär der Vereinigten Staaten eine kalibrierte Politik, öffentliche Anerkennung für bestimmte offensive Cyberoperationen zu erhalten. Abgesehen von Strafverfolgungsoperationen sind die öffentlichen Aufzeichnungen über Geheimdienst- und militärische Cyberoperationen an zwei Extremen ausgerichtet: spektakuläre Leaks (wie Vault 7155 und die Snowden Leaks) und öffentliche Ankündigungen von USCYBERCOM-Aktivitäten mit wenigen öffentlichen Details. Durchdachte, beweisgestützte Transparenz würde 1) die abschreckende Wirkung verbessern, 2) die staatliche Verantwortung und Aufsicht über solche Operationen klären, 3) internationalen Verbündeten und Partnern signalisieren, dass die Regierung Operationen im Cyberspace zugibt (besonders wichtig, falls ein autorisierter privater Akteur in Zukunft einen Fehler begeht), und 4) ein klareres Nachfragesignal an den privaten Sektor und verbündete Partner senden, welche Fähigkeiten geschätzt werden und warum. Wie ein Teilnehmer es formulierte: „Wenn die Bereitschaft besteht, öffentlicher über [offensive Cyber-Aktivitäten] zu sprechen und sie häufiger einzusetzen, wird die Marktreaktion tatsächlich deutlich stärker sein.“156

2. Schaffen Sie durch Pilotprogramme und Beschleuniger eine robuste offensive Cyber-Fähigkeitspipeline

Die Vereinigten Staaten kämpfen darum, die Kapazitäten qualifizierter kleinerer Unternehmen zu erhalten, und verlassen sich auf Hauptauftragnehmer mit belastenden Gemeinkosten oder maßgeschneiderten Dienstleistungsverträgen. Die Schaffung von Beschleunigern und Finanzierungsprogrammen speziell für offensive Cyberangriffe (in allen Formen) würde die Technologieanbieter dazu bewegen, Plattformen statt maßgeschneiderter Dienste anzubieten.

Für traditionellere, anspruchsvollere offensive Cyber-Fähigkeiten könnten Vulnerability Research Accelerators (VRAs) der Defense Innovation Unit (DIU) das Angebot an Zero-Day-Exploits deutlich erhöhen, insbesondere wenn die Accelerators den Einsatz künstlicher Intelligenz und Automatisierung im gesamten Prozess fördern. Die Schaffung zusätzlicher DOW-Richtlinien, um

Weg von mehrjährigen Serviceverträgen und hin zu mehr Other Transaction Authorities wird hier unabdingbar sein.

Für plattformorientierte Ansätze mit geringem Eigenkapital sollte die US-Regierung das Anduril-Modell für offensive Cyberangriffe. Anduril erhielt seinen ersten Auftrag über staatliche Pilotprogramme, die vom Innovationsteam des CBP entwickelt wurden.157 Auf der Finanzierungsseite wurde das Unternehmen sowohl von Risikokapitalgebern unterstützt als auch von Small Business Innovation Research-Programmen, um sein Geschäft auszubauen.158 In diesem Sinne sollten die FBI Operational Technology Division, das IDEAS-Programm und das Small Business Program der NSA159 sowie die DIU jeweils separat Pilotprogramme entwickeln, um mit kleinen Unternehmen an vorderster Front der offensiven Cybersicherheit zusammenzuarbeiten. Die Schaffung zusätzlicher DARPA SBIR (Small Business Innovation Research)160- Programme für offensive Cybersicherheit wird ebenfalls entscheidend sein, um sicherzustellen, dass Plattformen gebaut werden, die den Missionsanforderungen entsprechen.161

Angewandt auf offensives Cyber-Kriminalität bietet das Anduril-Modell die Möglichkeit, eine kleine Es gibt eine große Anzahl von langlebigen, produktorientierten Unternehmen, die ihr Betriebstempo an die Anforderungen der Regierung anpassen können. Dies macht den Markt auch für Investoren attraktiver: Risikokapitalgeber werden sich wohler fühlen, wenn es ein Produkt mit wiederkehrenden Einnahmen und einer skalierbaren Plattform gibt.

3. Investieren Sie in die Forschung zum Softwareverständnis

Um die nationale Wettbewerbsfähigkeit im offensiven und defensiven Cyberbereich langfristig zu sichern Um die Betriebsabläufe zu optimieren, sollte die US-Regierung nachhaltige Investitionen in die Forschung zum „Softwareverständnis“ priorisieren. Softwareverständnis, abgeleitet aus der Theorie der seltsamen Maschinen, umfasst nicht nur das Erkennen von Schwachstellen; es geht vielmehr darum zu verstehen, wie sich Systeme bei unerwarteten Eingaben verhalten und wie sich neu auftretende Computerzustände kontrollieren, stören oder abwehren lassen. Dieses Feld bildet die Grundlage sowohl für die Entwicklung von Exploits als auch für fortgeschrittene Verteidigungsanalysen, doch US-Forschungseinrichtungen sind in diesem Bereich nach wie vor chronisch unterfinanziert und unterentwickelt.

Um diesem Problem zu begegnen, sollten die USA ein Koalitionsmodell für Finanzierung und Koordination etablieren, das DARPA, NSF, NIST und führende akademische Institutionen in einem gemeinsamen Konsortium für offensive Cyber-Forschung zusammenführt. Dieses Modell würde die Entwicklung neuer Forschungsergebnisse von der Theorie zum Prototyp beschleunigen, und zwar durch eine Kombination aus Rapid-Prototyping-Fördermitteln, offenen Kooperationsrahmen und Mikrostipendien im DARPA-Stil für unabhängige Forscher und kleinere Labore. Das Programm sollte den Schwerpunkt auf Fördermittel mit geringem Aufwand und hoher Geschwindigkeit legen, um unkonventionelle, kreative Arbeit in Bereichen wie der automatisierten Exploit-Erkennung, binären Analysetools, der Schwachstellenforschung mit Large Language Models (LLM) und der Verhaltensanalyse komplexer Systeme zu unterstützen.

Diese Koalition sollte auch Anreize für Forschung schaffen, die den Gegnern Kosten auferlegt, ohne illegale Eingriffe, wie etwa die Nutzung von LLM-gestütztem Scambaiting162, die programmgesteuerte Analyse internationaler Standards und Versuche, Sicherheitsvorkehrungen durch Normungsgremien zu umgehen,

sowie andere Methoden zur Analyse gegnerischer Ökosysteme im großen Maßstab.

4. Genehmigung eines Pilotprogramms für den Zugang des privaten Sektors gegen Akteure mit geringem Risiko

Damit die US-Regierung skalierbare, offensive Cyber-Zugriffe vorantreiben kann, benötigt das Ökosystem eine ausgewogene Verteilung der Haftung zwischen staatlichen und privaten Akteuren, abgesichert durch Entschädigungen und definierte Safe Harbors, die eine begrenzte, überprüfbare Risikobereitschaft ermöglichen und gleichzeitig Kollateralschäden minimieren. Damit private Unternehmen in diesem Bereich wachsen können, müssen solche Forderungen öffentlich genug sein, um das Vertrauen von Unternehmen und Investoren zu stärken, und ausreichend reguliert sein, um Marktstabilität zu gewährleisten.

Während einige Programme durch einseitige Exekutivmaßnahmen durchgeführt werden könnten, hat der Kongress die Möglichkeit, neue Gesetze zu verabschieden, um die erforderlichen neuen Befugnisse, Modelle gemeinsamer Haftung und einen Weg für eine genehmigte Zusammenarbeit zu schaffen.163 Eine Möglichkeit, wie ein erstes Programm funktionieren könnte, sieht wie folgt aus:

Öffentliche Prämien für den Zugang (Belohnungen für Gerechtigkeit mit Biss)

Die USA sollten innerhalb der NSA und des DOJ/FBI Pilotprogramme mit begrenztem Umfang schaffen, die schafft einen rechtlichen und operativen Spielraum für geprüfte Cyberoperationen des privaten Sektors. Diese Operationen würden sich gegen Akteure mit geringem Risiko richten: eine begrenzte Anzahl von Akteuren, die sich derzeit der Strafverfolgung entziehen, in großem Maßstab schwer zu bekämpfen sind, aber keinen Einfluss auf langfristige Geheimdienst- oder Militäroperationen haben (z. B. Schweineschlachtbetrug, E-Crime-Wallets, Ransomware-Infrastruktur, eindeutig illegale Kryptogeldwäschefirmen in China und bestimmte ausländische terroristische Medienoperationen164). Das Programm muss öffentlich und nicht geheim sein, um die Vorteile des privaten Sektors wirklich zu nutzen.

Der operative Umfang muss eng begrenzt sein - dieses Pilotprojekt würde private Maßnahmen auf geringe gefährden ausländische kriminelle Ziele oder Ziele, die die nationale Sicherheit gefährden. Die Teilnehmer merkten an, dass Cyber-Akteure, gegen die zivilrechtliche Urteile oder Anklagen vorliegen, bereits den Anfang einer ersten Liste bilden könnten.165 Das Pilotprogramm würde zudem Verbindungen zu den Strafverfolgungsbehörden benötigen, um Sicherheitsunterstützung zu gewährleisten, insbesondere wenn bestimmte Akteure versuchen, sich an den privaten Teilnehmern zu rächen. Dieses Risiko ließe sich zudem minimieren, indem gezielt Ziele ausgewählt werden, die in den USA operierenden Personen kaum körperlichen Schaden zufügen können.

Nachdem der Regierung ein erster Zugang gewährt und genügend Beweise vorgelegt wurden, um dies zu bestätigen Der Zugriff erfolgt auf ein bestimmtes Ziel, die Rolle des privaten Betreibers endet, und die US-Regierung bleibt weiterhin aktiv. Nach erfolgreicher Validierung des Zugriffs kann die Regierung dem privaten Akteur einen Zuschuss oder eine Auszahlung gewähren. Damit die US-Regierung jedoch effektiv als „Trigger-Puller“ agieren kann, benötigen NSA und FBI zusätzliche Kapazitäten, um gegen Zugriffe vorgehen zu können.

und sich rechtzeitig mit den Partnern abzustimmen: Beide Organisationen müssten entsprechend personell ausgestattet sein und könnten zu diesem Zweck eine Task-Force-Struktur schaffen. Darüber hinaus müssten standardisierte Vertragsvorlagen, Beweisketten und Handoff-Playbooks erstellt werden, damit das Modell skalierbar ist, ohne dass jedes Mal neue Ad-hoc-Rechtsarbeiten anfallen.

Kritiker könnten argumentieren, dass ein Programm für den Zugang (ganz zu schweigen von den Effekten, wie unten erwähnt) Dies stellt eine Abweichung von internationalen Normen oder eine Verletzung der Souveränität dar. Dies ist jedoch irreführend, da der Zugang bereits weltweit von privaten Akteuren gekauft und geschaffen wird.
Darüber hinaus ist der Schaden, der der US-Souveränität bereits jetzt entsteht, real: Zehntausende Zivilisten und Unternehmen werden täglich Opfer transnationaler Cyberkriminalität, ganz zu schweigen von den Cyberaktivitäten nationaler Staaten. Untätigkeit, weil die rechtlichen Instrumente langsam sind oder das politische Risiko unbequem ist, verursacht realen, messbaren Schaden.

Bei einem Pilotprogramm für den Zugang ergeben sich zwei weitere Probleme: Erstens bräuchte der Privatsektor einen zivil- und strafrechtlichen Schutz vor anderen gesetzlichen Regelungen, der über den Ausnahmetatbestand für illegale Aktivitäten in der aktuellen Fassung hinausgeht. Zweitens besteht die Gefahr, dass die Exekutive den Privatsektor beauftragt, in ihrem Namen gegen das Gesetz zu verstoßen – ob versehentlich oder nicht. Die Beteiligung des Privatsektors an illegalen Aktivitäten muss klar überwacht und mit gesetzlichen Konflikten in Einklang gebracht werden.
zwischen ECPA (das die Datenfreigabe durch Dienstanbieter beschränkt), FISA (das eine Überwachungsaufsicht vorschreibt), Durchsuchungsbefehlsanforderungen für auf US-amerikanischem Boden durchgeführte Durchsuchungen und Verpflichtungen aus dem MLAT-Vertrag (sofern zutreffend).

Schutzmaßnahmen gegen diese Probleme lassen sich wahrscheinlich bereits durch einseitige Exekutivmaßnahmen schaffen: Zum Schutz vor Haftung könnten FBI und NSA das Pilotprogramm als autorisierte Geheimdienstaktivität gemäß CFAA bekannt geben (und damit alle Teilnehmer gemäß § 1030(f) öffentlich schützen). Dies würde den privaten Sektor jedoch wahrscheinlich nicht vor DMCA- oder anderen zivilrechtlichen Ansprüchen Dritter schützen. Schutzmaßnahmen gegen versehentliche Verstöße können teilweise durch die Gestaltung des Pilotprogramms gelöst werden: durch die richtige Zielauswahl durch die Exekutive, die Bestätigung des privaten Akteurs, dass er bei der Durchführung dieser Aktivität alle Bundesgesetze einhält, oder die Möglichkeit für den privaten Akteur, vor Erhalt des Zugriffs eine Überprüfung durch CONOP zu beantragen.

Die Teilnehmer des Runden Tisches waren sich nicht einig, ob für ein erfolgreiches Pilotprogramm Maßnahmen des Kongresses notwendig wären. Der Kongress hat jedoch die Möglichkeit, zusätzlichen Haftungsschutz für den privaten Sektor zu schaffen und gleichzeitig eine angemessene Aufsicht und Transparenz sicherzustellen.
Die Wiederbelebung früherer Gesetze, wie CISA 2015, könnte eine weitere Möglichkeit sein, den privaten Sektor vor Ansprüchen Dritter zu schützen: Der Rahmen für den Informationsaustausch CISA 2015 (der 2025 auslief) enthielt eine „No Cause of Action“-Klausel (d. h. Immunität vor Klagen jeglicher Art, zivil- oder strafrechtlich) für Unternehmen, die Indikatoren für Cyberbedrohungen weitergeben.166
Der Begriff „Indikator für Cyberbedrohungen“ wurde so weit gefasst (sogar einschließlich Schwachstellen), dass es möglich gewesen wäre, das Gesetz zum Schutz von Anbietern offensiver Fähigkeiten (oder sogar des Zugangs) im privaten Sektor zu nutzen.167
Eine Anforderung, dass das FBI und die NSA außerdem jährlich eine öffentliche, redigierte Bewertung des Pilotprojekts veröffentlichen, einschließlich der gewonnenen Erkenntnisse

und empfohlene Gesetzesänderungen könnten auch ein wirksamer Mechanismus für den Kongress, die Industrie und Verbündete sein, um zu beurteilen, ob das Programm ausgeweitet werden soll.

Krypto-Beschlagnahmungszugriffe – Ein erster Fall

Ein Pilotprogramm für den „Zugriff“ der Strafverfolgungsbehörden gegen Betrüger oder Diebe ausländischer Kryptowährungen könnte aus fünf Gründen der beste erste Anwendungsfall sein:

Erstens ist die Rechtslage bei der Beschlagnahmung ausländischer Kryptowährungen großzügiger als in anderen Fällen: Die Beschlagnahmung ausländischer Vermögenswerte wie Kryptowährungen ist einseitig möglich, erfordert aber entweder 1) die Unterstützung einer Kryptowährungsplattform168 oder 2) den bereits bestehenden Besitz des privaten Schlüssels des ausländischen Vermögenswerts.169 Während in einigen Fällen ein hinreichender Tatverdacht dafür besteht, dass die Vermögenswerte auf Erträge aus einer Straftat zurückzuführen sind,170 gilt der vierte Verfassungszusatz nicht für die Durchsuchung und Beschlagnahmung von Eigentum eines Ausländers ohne Wohnsitz im Ausland durch US-Beamte.171

Zweitens besteht bereits ein großes Interesse seitens des privaten Sektors, dies zu tun. Im Internet gibt es bereits zahlreiche „Scambaiting“-Communitys, in denen Sicherheitsforscher Betrüger mit verschiedenen Methoden „austricksen“.172 Wenn Scambaiter die Grenze zu illegalen Aktivitäten überschreiten, indem sie Webcams oder Betrugsanlagen hacken, fehlt es den Strafverfolgungsbehörden in der Vergangenheit an der Bereitschaft, gegen diese Personen vorzugehen.173 Auch Geschworene werden wahrscheinlich keine Person oder Organisation verurteilen, die gegen einen Cyberkriminellen vorgeht.174

Drittens steht dieser Fall am ehesten im Einklang mit der aktuellen Wirtschafts- und nationalen Sicherheitspolitik der USA.175 Während die USA versuchen, die „Kryptohauptstadt der Welt“ zu werden, bedrohen Akteure, die die Stabilität digitaler Vermögenswerte durch groß angelegte Raubüberfälle und Betrügereien beeinträchtigen, gleichzeitig die Stabilität des Kryptomarktes.176 Das Justizministerium hatte bisher unglaublichen Erfolg bei der Beschlagnahmung ausländischer Vermögenswerte. Da die Cyberkriminalität jedoch weiter zunimmt, werden die Cyberkriminellengruppen weiterhin Kryptowährungen (und insbesondere nicht gehostete Wallets) verwenden, was eine Beschlagnahmung in großem Umfang ohne die Unterstützung des privaten Sektors erschweren könnte, entweder weil es zu viele Kriminelle oder Wallets gibt177 oder weil die Wallets selbst schwer zu knacken sind.178 Die bisher größte Beschlagnahmung von Kryptowährungen zielte auf lediglich 6 nicht gehostete Wallets ab (wobei eine rekordverdächtige Beschlagnahmung von 15 Milliarden Dollar erfolgte). Allerdings zeigen FBI-Berichte, dass jedes Jahr 10 bis 16 Milliarden Dollar durch Krypto-Betrug aus den USA abfließen, der mit einer schwindelerregenden Zahl von Wallets in Verbindung steht.179 Aktuelle Berichte deuten darauf hin, dass Kryptowährungen im Wert von über 75 Milliarden Dollar in der Blockchain mit kriminellen Aktivitäten in Verbindung stehen, wobei über 40 Milliarden Dollar mit Betreibern und Anbietern von Darknet-Märkten in Verbindung stehen.180

Viertens dürften private Kapitalgeber und Unternehmen leichter feststellen können, wie sie die

Markt für ein solches Strafverfolgungsprogramm, da die Strafverfolgungsbehörden von den Organisationen, die derzeit Cyberoperationen durchführen, die wenigsten Geheimnisse preisgeben.

Und schließlich sind Organisationen, die normalerweise gegen Cyberangriffe des privaten Sektors sind, in Bezug auf Kryptodiebstahl stärker auf einer Linie: Anders als traditionelle Big-Tech-Unternehmen werben Kryptowährungsplattformen aggressiver um die Unterstützung des privaten Sektors, um Akteure der Internetkriminalität auszuschalten, und bieten dafür sogar Kopfgelder an.181 Risikokapitalfirmen haben ebenfalls stark in Kryptowährungen investiert und würden wahrscheinlich Unternehmen finanzieren, die ihre Investitionen zusätzlich schützen.182

Die Schaffung eines Programms, mit dem ein Akteur nach einer erfolgreichen Beschlagnahmung 33 % des Wallet-Inhalts zurückerhalten könnte, würde einen Großteil der verlorenen Kryptowährungen wieder in die US-Wirtschaft zurückführen und gleichzeitig eine neue erfolgreiche Heimindustrie schaffen. Wenn private Betreiber nachweislich die Kontrolle über Erträge aus Straftaten erlangen (z. B. über die Seed-Phrase eines Krypto-Wallets oder den Zugriff auf private Schlüssel), muss das Justizministerium die Prozesse optimieren, um Beschlagnahmungen oder gegebenenfalls gegenseitige Rechtshilfe zu gewährleisten. Laut einem ehemaligen Teilnehmer eines Runden Tisches mit der Regierung hat das Justizministerium Beschlagnahmungsbefehle innerhalb von 24 Stunden nach Erhalt der Seed-Phrase einer Wallet erwirkt183 - um sicherzustellen, dass dieses Tempo auch dann eingehalten wird, wenn die Anzahl der Zugriffe zunimmt, sind dies der Schlüssel zum Erfolg eines Programm Erfolg.

Da jedes Zugangsprogramm mit einer Prämie perverse Anreize schaffen könnte (z. B. den Diebstahl von Kryptowährungen mit einer Wallet, um dies dann den Strafverfolgungsbehörden zu melden und so eine Auszahlung von 5 % zu garantieren), müsste das Justizministerium außerdem sicherstellen, dass das nicht klassifizierte und öffentliche Programm weiterhin über ein Antragsverfahren verfügt, bei dem der Antragsteller der Überwachung seiner Ausgabegewohnheiten und seines Vermögens zustimmt.

Die Schaffung eines solchen Zugangsprogramms könnte auch den privaten Sektor und Regierungen weltweit dazu bewegen, kriminelle Aktivitäten zu unterbinden, einfach weil sie nicht wollen, dass die USA ein solches Programm in ihren Systemen oder Unternehmen einsetzen. Ein Großteil des Cyberscam-Bereichs ist auf wohlgesonnene Regierungen und große Technologieinfrastrukturen angewiesen (wo Betrügerfarmen bereits gegen die Geschäftsbedingungen von Technologieunternehmen verstoßen). Die Schaffung eines öffentlichen Programms könnte an sich Druck auf derzeit widerspenstige Plattformen und Regierungen ausüben.

Direkte, öffentliche Beauftragung von Vertrauenspersonen

Ein öffentliches Deputationsregime, das eine kleine Liste geprüfter Unternehmen erstellt, um begrenzte, staatlich autorisierte Störaktionen durchzuführen, könnte die Skalierung offensiver Cyberangriffe ermöglichen, während

Einbindung von Verantwortlichkeit, Überprüfbarkeit und Aufsicht. Dies ist keine freizügige „Hackback“-Lösung: Die Teilnehmer der Diskussionsrunde waren sich einig, dass unbegrenzte, unregulierte Vergeltungsmaßnahmen gefährlich und kontraproduktiv wären. Stattdessen würde das Pilotprojekt eine kleine Liste vertrauenswürdiger Unternehmen (die wahrscheinlich bereits durch frühere Operationen oder das oben genannte Pilotprogramm das nötige Vertrauen aufgebaut haben) gegen eine von der Regierung festgelegte Reihe von Zielen einsetzen. Die Regierung würde explizite Schutz- und Haftungsteilungsvereinbarungen treffen, damit diese Unternehmen begrenzte, gesetzlich autorisierte Störungsmaßnahmen zur Unterstützung der Strafverfolgung oder der nationalen Sicherheit durchführen können.

Aus Programmsicht müsste die US-Regierung ausreichend Aufsicht schaffen, um sicherzustellen, dass jeder private Effekt gezielt und vertretbar generiert wird. Da Vertrauen im Mittelpunkt des Modells steht, würden die beauftragten Stellen einer strengen Überprüfung unterzogen (Sicherheitsüberprüfungen, Hintergrundüberprüfungen und vertragliche Verpflichtungen zur Geheimhaltung und zum kontrollierten Umgang mit Geschäftsgeheimnissen), anstatt wie oben dargestellt auf dem öffentlichen Markt zu agieren. Private Akteure, die die Überprüfung bestehen, sollten in der Lage sein, Effekte opportunistisch zur Genehmigung vorzuschlagen.

Die Teilnehmer des Runden Tisches schlugen zwei Möglichkeiten vor, wie eine solche Delegation oder Lizenzierung erfolgen könnte:

1) **Präsidialdirektive / Militärische Vertretung:**

Eine präsidiale Direktive könnte CYBERCOM dazu auffordern, private Akteure mit der Bekämpfung von APT-Gruppen mit geringerem Risiko zu beauftragen, die eine Bedrohung für DODIN darstellen. Dies könnte als Notlösung oder Ergänzung für Cyber-Force-Initiativen dienen, während CYBERCOM seine eigenen Kapazitäten aufbaut und gleichzeitig private Akteure in CYBERCOM-Prozesse sowie die behördenübergreifende oder internationale Koordination integriert. Um inländische und ausländische Aktivitäten zu trennen, müsste ein solches Programm gegebenenfalls die Weitergabe inländischer Zugriffe und den Informationsaustausch an die Bundespolizei beinhalten. Die öffentliche Aufsicht über solche Akteure wäre bei solchen Behörden jedoch wahrscheinlich eingeschränkt.

2) **Cyber-Kaperbriefe oder andere gesetzliche Lizenzierungsregelungen**

Der Kongress könnte einen Lizenzrahmen – basierend auf den Grundsätzen des Paragraphen 1030(f)/CFAA oder einem neuen eigenständigen Gesetz – verabschieden, der bestimmte Arten von ansonsten illegalen Computerzugriffen und -störungen ausdrücklich erlaubt, sofern diese im Rahmen eines von der Regierung genehmigten Auftrags und entsprechender Einsatzregeln erfolgen. Die Teilnehmer der Diskussionsrunde waren sich weitgehend uneinig, ob ein solches Vorgehen des Kongresses sinnvoll oder realistisch wäre.
Eine vom Kongress ausgearbeitete Gesetzgebung wäre jedoch eine Möglichkeit, das von Akteuren des privaten Sektors geforderte Gleichgewicht zwischen Transparenz und Kontrolle herzustellen und gleichzeitig einen neuen Rahmen zu schaffen, der nicht durch verdeckte Geheimdienstkulturen, unterentwickelte Militärplattformen oder die begrenzte Autorität der Strafverfolgungsbehörden eingeschränkt wäre.

Abschluss

Die USA haben die Chance, im offensiven Cyber-Bereich vom Ad-hoc- zum Architektur-Prinzip überzugehen. Dazu müssen sie einen kohärenten Rahmen schaffen, der die ad hoc und persönlichkeitsgesteuerte Koordination in ein dauerhaftes System nationaler Kapazitäten verwandelt. Die Lücken sind offensichtlich: Die unterentwickelte, undurchsichtige Rechtsstruktur der USA hemmt die Initiative des privaten Sektors, das zersplitterte staatliche Ökosystem kann mit den neuen Bedrohungen nicht Schritt halten, und die Forschungslandschaft der USA unterschätzt das Verständnis von Software – die Grundlage offensiver wie defensiver Innovationen.

Doch die Chancen liegen auf der Hand. Die USA verfügen über eine beispiellose Kombination aus privatem Know-how, technischem Talent und frei fließendem Kapital. Eine nationale offensive Cyberstrategie, die akzeptables Verhalten definiert, eine konsistente Nachfrage signalisiert, die Koordination der Verbündeten stärkt und legale Kanäle für private Beteiligung schafft, würde es der Regierung ermöglichen, schnell und verhältnismäßig zu handeln und gleichzeitig Rechenschaftspflicht und Kontrolle zu wahren. Durch Investitionen in Pilotprogramme, die Beschleunigung der Forschung zum Verständnis von Software und die Schaffung gesetzlicher oder exekutiver Mechanismen zur sicheren Beauftragung vertrauenswürdiger privater Partner mit Zugriff (oder sogar Auswirkungen) können die USA ein neues Modell für verantwortungsvolles Handeln umsetzen.

Letztendlich verfügt Amerika über die erforderlichen Fähigkeiten, es muss nur das Chaos beseitigen, das es umgibt. Die Herausforderung für die Politik besteht nicht darin, neue Talente oder Technologien zu entwickeln, sondern die rechtliche, institutionelle und marktwirtschaftliche Infrastruktur zu schaffen, die Wachstum ermöglicht. Der Aufbau dieses Rahmens ermöglicht einen agileren, ethischeren und skalierbareren Ansatz für offensive Cyber-Macht – einen Ansatz, der demokratische Werte widerspiegelt und gleichzeitig nationale Interessen schützt. Kurz gesagt: Schaffen Sie den Rahmen, und die Kapazitäten werden folgen.

Über die Autoren

Winnona DeSombre Bernsen ist Nonresident Fellow des Atlantic Council und Gründerin der Konferenz DistrictCon für offensive Sicherheit. Sie hat einen Master of Public Policy der Harvard Kennedy School und einen Juris Doctor der Georgetown Law School. Winnona war zuvor Sicherheitsingenieurin bei Googles Threat Analysis Group und verfolgte dort gezielte Bedrohungen gegen Google-Nutzer. In den letzten Jahren hat Winnona Inhalte für Hackerkonferenzen organisiert (u. a. als Moderatorin bei den Pwnie Awards) und mehrere Artikel zur Verbreitung offensiver Cyber-Fähigkeiten verfasst.

Sergey Bratus ist Professor für Cybersicherheit, Technologie und Gesellschaft am Dartmouth College und außerordentlicher Professor für Informatik. Von 2018 bis 2024 war er Programmmanager im Information Innovation Office (I2O) der DARPA, wo er mehrere grundlegende Forschungsprogramme zu Cybersicherheit, Resilienz und der Aufrechterhaltung kritischer Software entwickelte. Sergey interessiert sich für die Identifizierung und Beseitigung der Ursachen von Softwareschwachstellen und ist davon überzeugt, dass dies die Verbindung von modernstem Hacking mit grundlegenden Konzepten der Informatik erfordert. Er ist überzeugt, dass sich modernstes Hacking zu einer eigenständigen Disziplin der Informatik entwickelt hat, auch wenn es nicht formal als solche anerkannt ist, und dass dessen Erforschung für die Entwicklung zukünftiger Computersysteme, denen wir endlich vertrauen können, unverzichtbar ist.

Danksagung

Die Autoren möchten Dartmouth ISTS für die Ausrichtung des Runden Tisches danken, und den Teilnehmern die zum Roundtable in Dartmouth kamen, wertvolle Einblicke lieferten und Feedback zu nachfolgenden Papierentwürfen gaben. Ein besonderer Dank gilt Mary Brooks: Ohne ihre redaktionelle und moderierende Unterstützung vor, während und nach dem Roundtable wäre dieses Papier nicht zustande gekommen.

Endnoten

[1] John Sakellariadis, *Republikaner wollen, dass US-Unternehmen gegen China vorgehen.* POLITICO Pro, Juni 9, 2025. https://subscriber.politicopro.com/article/2025/06/republicans-want-us-companies-to-hack-back-against-china-00394646

2David Dimolfetta. *Auftragnehmer könnten Gegner mit Hacks zurückschlagen, sagt führender Cyber-Demokrat.* Nextgov/FCW, 2. April 2025. https://www.nextgov.com/cybersecurity/2025/04/contractors-could-hack-back-against-adversaries-top-cyber-democrat-says/404233/

[3] Greg Otto. *Der Leiter des Cyber-Sicherheitsrats des Nationalen Sicherheitsrats will offensive Operationen „normalisieren“.* CyberScoop, 1. Mai 2025. https://cyberscoop.com/alexei-bulazel-white-house-national-security-council-destigmatize-offensive-cyber-rsac-2025/

[4] Sezaneh Seymour, Brandon Wales. *Partner oder Provokateure? Beteiligung des Privatsektors an offensiven Cyberoperationen.* Lawfare, 16. Juli 2025. https://www.lawfaremedia.org/article/partners-or-provocateurs-- Beteiligung des privaten Sektors an offensiven Cyber-Operationen

[5] Matt Seldon. *Emily Goldman wird dem Cyber-Büro des Nationalen Sicherheitsrats beitreten.* HSToday, 10. März 2025. https://www.hstoday.us/subject-matter-areas/cybersecurity/emily-goldman-set-to-join-national-security-councils-cyber-office/

[6]Cyber Persistence Theory, geprägt von Michael P. Fischerkeller, Emily O. Goldman und Richard J. Harknett erklärte 2022, der Schlüssel zur Sicherheit im Cyberspace liege in proaktiven Operationen und Kampagnen, die Schwachstellen identifizieren, deren Ausnutzung verhindern und Schadensbegrenzung ermöglichen. Greg Otto. *Amerikas Verbündete ändern ihre Haltung: Im Cyberspace geht es um Beständigkeit, nicht um Abschreckung.* CyberScoop, 2. Oktober 2024. https://cyberscoop.com/cybersecurity-deterrence-persistence-richard-harknett-dod-strategy/

[7] „Im Jahr 2018 verlagerten sich die strategischen Leitlinien der USA in der Nationalen Sicherheitsstrategie der Vereinigten Staaten von Amerika (NSS) dahingehend, die Bedeutung dieses Wettbewerbsraums hervorzuheben, und USCYBERCOM verordnete einen strategischen Ansatz des anhaltenden Engagements.“ Michael P. Fischerkeller et. al., *Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation.* The Cyber Defense Review. 2019. Abgerufen am 14. Oktober 2024, https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf

8USCYBERCOMs Strategie des anhaltenden Engagements (die vor der Cyber Persistence Theory angekündigt wurde, aber viele der gleichen Konzepte anwendet) führte zu Vorwärtsoperationen in der Ukraine, bei denen Cyber-Operatoren ständig daran arbeiten, Cyber-Bedrohungen abzufangen und zu stoppen und gleichzeitig die Fähigkeiten der Gegner zu schwächen. Michael Fischerkeller, Emily Goldman, Richard Harknett. *Cyber-Persistenz-Theorie im russisch-ukrainischen Krieg.* Binding Hook. 7. November 2023. https://bindinghook.com/cyber-persistence-theory-in-the-russo-ukrainian-war/. US Cyber Command PAO. *CYBER 101 – Vorwärtsverteidigung und anhaltendes Engagement.* US Cyber Command, 25. Oktober 2022. https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/

[9] Greg Otto. *Der Leiter des Cyber-Sicherheitsrats des Nationalen Sicherheitsrats will offensive Operationen „normalisieren“.* CyberScoop, 1. Mai 2025. https://cyberscoop.com/alexei-bulazel-white-house-national-security-council-destigmatize-offensive-cyber-rsac-2025/

10Weltweiter Marktanteil von Desktop-PCs und Mobilgeräten. StatCounter Global Stats. Abgerufen am 7. Oktober 2025 von https://gs.statcounter.com/platform-market-share/desktop-mobile/worldwide/2010

[11] *Komplexität tötet Softwareentwickler.* InfoWorld. Abgerufen am 7. Oktober 2025 von https://www.infoworld.com/article/2270714/complexity-is-killing-software-developers.html

[12] Winnona DeSombre Bernsen. *Crash (exploit) and burn: Sicherung der offensiven Cyber-Lieferkette zur Bekämpfung Chinas im Cyberspace.* Atlantic Council, 25. Juni 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/

[13] Sergey Bratus et al. *Exploit-Programmierung: Von Pufferüberläufen zu „seltsamen Maschinen“ und Berechnungstheorie.* Langsec, Dezember 2011. Abgerufen am 7. Oktober 2025 von https://langsec.org/papers/Bratus.pdf

[14] Ian Beer. *Blasting Past Webp: Eine Analyse des NSO BLASTPASS iMessage-Exploits.* Google-Projekt Zero, 26. März 2025. https://googleprojectzero.blogspot.com/2025/03/blasting-past-webp.html

15Ben Hawkes. *Der WebP-0day.* Icosceles, 21. September 2023. https://blog.isosceles.com/the-webp-0day/

[16] Ian Beer & Samuel Groß. *Ein tiefer Einblick in einen NSO Zero-Click iMessage-Exploit: Remote Code Execution.* Project Zero, 15. Dezember 2021. https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html

[17] Sergey Bratus et al. *Exploit-Programmierung: Von Pufferüberläufen zu „seltsamen Maschinen“ und Berechnungstheorie.* Langsec, Dezember 2011. Abgerufen am 7. Oktober 2025 von https://langsec.org/papers/Bratus.pdf

[18] Sergej Bratus. *Was mich die Hackerforschung gelehrt hat.* Dartmouth College. Abgerufen am 7. Oktober 2025 von https://www.cs.dartmouth.edu/~sergey/hc/rss-hacker-research.pdf

[19] Winnona DeSombre Bernsen. *Crash (exploit) and burn: Sicherung der offensiven Cyber-Lieferkette zur Bekämpfung Chinas im Cyberspace.* Atlantic Council, 25. Juni 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/. Bestätigt durch Dartmouth ISTS Offensive Cyber Roundtable, Anmerkung eines aktuellen Branchenteilnehmers, 3. Oktober 2025.

[20] Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines aktuellen Branchenteilnehmers, 3. Oktober 2025.

[21] DARPA hat massiv in die KI-gestützte Erstellung von Exploit-Ketten sowie in die automatisierte Identifizierung und Behebung von Schwachstellen investiert. Obwohl der Fokus auf der Defensive liegt, präsentierte der DARPA AIxCC-Wettbewerb mehrere Teams, die mithilfe von KI-Systemen wertvolle Fehlerberichte und Patches erstellen konnten. Die Patches wurden in durchschnittlich 45 Minuten eingereicht, wobei die Kosten pro Aufgabe durchschnittlich 152 US-Dollar betrugen. Während das Einreichen von Patches eindeutig eine defensive Aktivität ist, hat die Identifizierung von Schwachstellen einen doppelten Nutzen und könnte auch für offensivere Zwecke eingesetzt werden. *Die AI Cyber Challenge markiert einen entscheidenden Wendepunkt für die Cyberabwehr.* DARPA, 8. August 2025). Abgerufen am 7. Oktober 2025 von https://www.darpa.mil/news/2025/aixcc-results

[22] Mark Ellzey. *Verwendung von Censys zum Auffinden falsch konfigurierter S3-Systeme.* Censys, 3. Januar 2023. Abgerufen am 7. Oktober 2025. von https://censys.com/blog/using-censys-to-find-misconfigured-s3

[23] Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen von aktuellen Teilnehmern aus der Industrie, der Wissenschaft, der ehemaligen Regierung und der aktuellen Regierung, 3. Oktober 2025.

[24] Haushaltsvoranschläge des Verteidigungsministeriums für das Haushaltsjahr 2026. US Cyber Command. Abgerufen am 6. Oktober 2025 von https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/03_RDT_and_E/RDTE_CYBERCOM_PB_2026.pdf

[25] Jamie Levy, Lindsey O'Donnell-Welch, Michael Tigges. *Ein Fehler eines Angreifers gab uns Einblick in seine Operationen.* Huntress, 9. September 2025. https://www.huntress.com/blog/rare-look-inside-attacker-operation

[26] Es ist wichtig zu beachten, dass Huntress weitgehend auf der Grundlage der Geschäftsbedingungen seiner Softwarelizenzen agierte. Ein so schneller Prozess könnte jedoch auch außerhalb der Softwarelizenzsysteme durchgeführt werden, wenn der Privatsektor ausreichend rechtlich abgesichert wäre.

[27] Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen von aktuellen Teilnehmern aus der Industrie und der Regierung, 3. Oktober 2025.

[28] Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen eines aktuellen Branchenteilnehmers, 3. Oktober 2025. 29

Google Threat Analysis Group. *Vom Iran unterstützte Gruppe verstärkt Phishing-Kampagnen gegen Israel und die USA* Google, 14. August 2024. https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/

[30] Microsoft Threat Intelligence. *Unterbinden Sie die aktive Ausnutzung lokaler SharePoint-Sicherheitslücken.* Microsoft Security Blog, 22. Juli 2025. https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

[31] Kongressforschungsdienste. 3. August 2022. *Überblick über die Regierungsmaßnahmen im Rahmen der Gesetz über gespeicherte Kommunikation (SCA).* CRS-Berichtsnummer LSB10801. https://www.congress.gov/crs-product/LSB10801

[32] DOJ-Büro für Öffentlichkeitsarbeit. *„LockerGoga“, „MegaCortex“ und „Nefilim“ Ransomware-Administrator Anklage wegen Ransomware-Angriffen.* US-Justizministerium, 9. September 2025. https://www.justice.gov/opa/pr/lockergoga-megacortex-and-nefilim-ransomware-administrator-charged-ransomware-attacks

[33] *„Vereinigte Staaten gegen ca. 225.364.961 USDT“,* Zivilklage Nr. 25-cv-1907. Bezirksgericht der Vereinigten Staaten Gericht für den District of Columbia. 18. Juni 2025. https://www.justice.gov/usao- dc/media/1403996/dl?inline

[34] Steven Masada. *Lumma-Diebstahl bekämpfen: Microsoft führt weltweite Maßnahmen gegen beliebtes Cybercrime-Tool an.* Microsoft On the Issues, 21. Mai 2025. https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/

[35] *Microsoft Corporation gegen DOES 1-10.* Fall Nr. 1:25-CV-2695-MHC. US-Bezirksgericht für Nördlicher Bezirk von Georgia, 15. Mai 2025. https://www.noticeofpleadings.net/lumma/files/06_CourtOrders/01_TRO%20Order%20and%20Order%20to%20Show%20Cause.pdf

[36] *Microsoft Corporation v. Does 1-10.* Fall Nr. 1:2025cv02695. US-Bezirksgericht für den Norden Bezirk Georgia, 13. Mai 2025. https://dockets.justia.com/docket/georgia/gandce/1:2025cv02695/343822

[37] Will Strafach. *Tycoon 2FA-Infrastrukturerweiterung: Eine DNS-Perspektive.* DNSFilter, 8. Juli 2025. https://www.dnsfilter.com/blog/tycoon-2fa-infrastructure-expansion

[38] Sezaneh Seymour, Brandon Wales. *Partner oder Provokateure? Beteiligung des Privatsektors an offensiven Cyberoperationen.* Lawfare, 16. Juli 2025. https://www.lawfaremedia.org/article/partners-or-provocateurs-- Beteiligung des privaten Sektors an offensiven Cyber-Operationen

[39] *Größte Social-Media-Plattformen nach Nutzern 2025.* Statista, 25. März 2025. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[40] Felix Richter. *Infografik: Die großen Drei bleiben im stetig wachsenden Cloud-Markt führend.* Statista-Tagesdaten, 21. August 2025. https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers

41Senator Ron Wyden. Brief an Christopher A. Wray, Direktor des FBI. Büro von Senator Ron Wyden, 20. Dezember 2022.

https://www.wyden.senate.gov/imo/media/doc/FBI%20Hacking%20Letter%20Signed%2012.20.22.pdf

42David DiMolfetta, *DOD erhält im Rahmen des Versöhnungspakets der Republikaner Millionen für Cyber-Fähigkeiten.* Nextgov/FCW, 7. Juli 2025. https://www.nextgov.com/cybersecurity/2025/07/dod-gets-millions-cyber-capabilities-under-gop-reconciliation-package/406540/

[43] Winnona DeSombre Bernsen. *Crash (exploit) and burn: Sicherung der offensiven Cyber-Lieferkette zur Bekämpfung Chinas im Cyberspace.* Atlantic Council, 25. Juni 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/

[44] Executive Order 14093: *Verbot der Verwendung kommerzieller Spyware durch die US-Regierung Das birgt Risiken für die nationale Sicherheit.* 88 FR 18957. Federal Register, 30. März 2023. https://www.federalregister.gov/documents/2023/03/30/2023-06730/prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to

[45] Haushaltsvoranschläge des Verteidigungsministeriums für das Haushaltsjahr 2026. US Cyber Command. Abgerufen am 6. Oktober 2025 von https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/03_RDT_and_E/RDTE_CYBERCOM_PB_2026.pdf

[46] Haushaltsvoranschläge des Verteidigungsministeriums für das Haushaltsjahr 2026. US Cyber Command. Abgerufen am 6. Oktober 2025 von

https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/03_RDT_and_E/RDTE_CYBERCOM_PB_2026.pdf

[47] Haushaltsvoranschläge des Verteidigungsministeriums für das Haushaltsjahr 2026. US Cyber Command. Abgerufen am 6. Oktober 2025 von https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/03_RDT_and_E/RDTE_CYBERCOM_PB_2026.pdf

[48] ANTRAG UND EIDESSTATTLICHE ERKLÄRUNG FÜR EINEN BESCHLAGNAHMEBEFEHL PER TELEFON ODER ANDEREN ZUVERLÄSSIGEN ELEKTRONISCHEN MITTELN. Fallnummer 2:23-MJ-4251. Bezirksgericht der Vereinigten Staaten, Zentralbezirk von Kalifornien, 23. August 2023. https://www.justice.gov/usao-cdca/file/1312086/dl?inline

[49] DIE RICHTLINIEN DES GENERALSTAATSANWALTS ZUR VERWENDUNG VON FBI-VERTRAULICHKEITEN HUMAN SOURCES. Justizministerium. Abgerufen am 6. Oktober 2025 von https://www.justice.gov/oip/foia-library/foia-processed/general_topics/ag_guidelines_FBI_human_confidential_sources_2/dl, verifiziert durch Dartmouth ISTS Roundtable durch einen Branchenteilnehmer, 3. Oktober 2025.

[50] Dartmouth ISTS Offensive Cyber Roundtable, Anmerkung eines Teilnehmers, 3. Oktober 2025.

[51] Amnesty International Security Lab. *Cellebrite-Zero-Day-Exploit greift Telefon eines serbischen Studenten an Aktivist.* Amnesty International. 28. Februar 2025. *Amnesty International Security Lab.* https://securitylab.amnesty.org/latest/2025/02/cellebrite-zero-day-exploit-used-to-target-phone-of-serbian-student-activist/

[52] Anmerkungen von Leonard Bailey, Panel on Offensive Cyber während der Konferenz des Center for Cybersecurity Policy and Law (Regisseur). 8. Oktober 2025. CyberNext DC 2025 [Videoaufzeichnung]. https://www.youtube.com/watch?v=VxtE68RcqXs

[53] *Vereinigte Staaten von Amerika, Kläger-Berufungsführer, gegen William Adderson Jarrett, Beklagter-Berufungsgegner, 338 F.3d 339 (4. Cir. 2003).* Justia Law. Abgerufen am 6. Oktober 2025 von https://law.justia.com/cases/federal/appellate-courts/F3/338/339/549971/

[54] *Vereinigte Staaten von Amerika, Kläger-Berufungsführer, gegen William Adderson Jarrett, Beklagter-Berufungsgegner, 338 F.3d 339 (4. Cir. 2003).* Justia Law. Abgerufen am 6. Oktober 2025 von https://law.justia.com/cases/federal/appellate-courts/F3/338/339/549971/

[55] Dartmouth ISTS Offensive Cyber Roundtable, Bemerkungen mehrerer ehemaliger und aktueller Regierungsvertreter Teilnehmer, 3. Oktober 2025.

[56] Colin Demarest. *RTX Cyber- und Intel-Geschäft wird nach dem Verkauf zu Nightwing.* C4ISRNET über Yahoo News, 1. April 2024. https://www.yahoo.com/news/rtx-cyber-intel-business-becomes-190451924.html

[57] *Nightwing Group 2025 Unternehmensprofil: Bewertung, Finanzierung & Investoren.* PitchBook. Abgerufen im Oktober 6, 2025, von https://pitchbook.com/profiles/company/539011-72

[58] *Lösungen – Nightwing* . Abgerufen am 6. Oktober 2025 von https://www.nightwing.com/solutions/index.html

[59] Haushaltsvoranschläge des Verteidigungsministeriums für das Haushaltsjahr 2026. US Cyber Command. Abgerufen am 6. Oktober 2025 von https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/03_RDT_and_E/RDTE_CYBERCOM_PB_2026.pdf

[60] Saber + cyb0rg. *APT Down – Die Nordkorea-Akten.* Phrack. Abgerufen am 9. Oktober 2025 von https://phrack.org/issues/72/7.html

[61] Clement Njoki. *Ethisches Scambaiting: Strategien, Herausforderungen und globale Lösungen verstehen.* GASA, 21. Mai 2024. https://www.gasa.org/post/ethical-scambaiting-understanding-strategies-challenges-and-global-solutions

[62] Andy Greenberg. *Nordkorea hat ihn gehackt. Deshalb legte er das Internet lahm.* WIRED, 2. Februar 2022. https://www.wired.com/story/north-korea-hacker-internet-outage/

[63] Anmerkungen von Meredith Burkardt, Panel on Offensive Cyber während des Center for Cybersecurity Policy and Law (Direktorin). 8. Oktober 2025. CyberNext DC 2025 [Videoaufzeichnung].

[64] Evan Wexler, Elias Mallette. *Wie die geheime Elite-Hacking-Einheit der NSA arbeitet.* FRONTLINE, 29. Mai 2014. https://www.pbs.org/wgbh/frontline/article/how-the-nsas-secret-elite-hacking-unit-works/

[65] Sam Biddle. *US-Geheimdienste erhalten eine zentrale Anlaufstelle für den Kauf Ihrer sensibelsten persönlichen Daten.* The Intercept, 22. Mai 2025. https://theintercept.com/2025/05/22/intel-agencies-buying-data-portal-privacy/

[66] Nicole Perlroth. *Die unerzählte Geschichte des amerikanischen Zero-Day-Marktes.* WIRED, 14. Februar 2021. https://www.wired.com/story/untold-history-americas-zero-day-market/

[67] Matan Mimran. *Die langfristigen Bedrohungen durch die Vault 7-Leaks.* Abgerufen am 8. Oktober 2025 von https://www.cybereason.com/blog/vault-7-leaks-long-term-threats

[68] *Leiter der Elite-Hacking-Einheit der NSA: Wie wir hacken.* ABC News, 28. Januar 2016. https://abcnews.go.com/International/head-nsas-elite-hacking-unit-hack/story?id=36573676

[69] Dartmouth ISTS Offensive Cyber Roundtable, Bemerkungen mehrerer ehemaliger und aktueller Regierungsvertreter Teilnehmer, 3. Oktober 2025.

[70] Ellen Nakashima. *„No Such Agency" spioniert die Kommunikation der Welt aus.* The Washington Post, 7. Juni 2013. https://web.archive.org/web/20130607162318/https://www.washingtonpost.com/world/national-security/no-such-agency-spies-on-the-communications-of-the-world/2013/06/06/5bcd46a6-ceb9-11e2-8845-d970ccb04497_story.html

[71] *Cybersecurity Collaboration Center.* Abgerufen am 9. Oktober 2025 von https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/. *Informationen zur NSA-Mission.* National Security Agency. Abgerufen am 9. Oktober 2025 von https://www.nsa.gov/about/

[72] Kim Zetter. *Countdown zum Zero Day.* Pentagon-Bibliothek. Abgerufen am 7. Oktober 2025 von https://pentagonlib.overdrive.com/media/1397159

[73] Dartmouth ISTS Offensive Cyber Roundtable, Bemerkungen mehrerer ehemaliger und aktueller Regierungsvertreter Teilnehmer, 3. Oktober 2025.

[74] Dartmouth ISTS Offensive Cyber Roundtable, Bemerkungen mehrerer ehemaliger und aktueller Regierungsvertreter Teilnehmer, 3. Oktober 2025.

[75] Winnona DeSombre Bernsen. *Crash (exploit) and burn: Sicherung der offensiven Cyber-Lieferkette zur Bekämpfung Chinas im Cyberspace.* Atlantic Council, 25. Juni 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/

[76] CYBER 101 – Mission des US Cyber Command. Abgerufen am 16. März 2025 von https://www.cybercom.mil/Media/News/Article/3192016/cyber-101-us-cyber-command-mission/ https%3A%2F%2Fwww.cybercom.mil%2FMedia%2FNews%2FArticle%2F3192016%2Fcyber-101-us-cyber-command-mission%2F

[77] Mark Pomerleau. *Das Cyber Command unterstützt Angriffe auf iranische Atomanlagen, doch Details werden geheim gehalten.* DefenseScoop, 23. Juni 2025. https://defensescoop.com/2025/06/23/cyber- command-supports-attack-iran-nuclear-facilities-midnight-hammer/

[78] Dina Temple-Raston. *Wie die USA ISIS gehackt haben.* NPR, 26. September 2019. https://www.npr.org/2019/09/26/763545811/how-the-us-hacked-isis. Alisa Chang, *Neu veröffentlichte Regierungsdokumente beschreiben die US-Cyberoffensive gegen ISIS.* NPR. 23. Januar 2020. https://www.npr.org/2020/01/23/799004239/newly-released-government-documents-detail-us-cyberoffensive-on-isis

[79] Haushaltsvoranschläge des Verteidigungsministeriums für das Haushaltsjahr 2026. US Cyber Command. Abgerufen am 6. Oktober 2025 von https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/03_RDT_and_E/RDTE_CYBERCOM_PB_2026.pdf

[80] Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines aktuellen Militärteilnehmers, 3. Oktober 2025.

[81] Robert Chesney, *Probleme gemäß Titel 10 und Titel 50, wenn Computernetzwerkoperationen Auswirkungen auf Drittländer haben.* Lawfare, 12. April 2018. https://www.lawfaremedia.org/article/title-10-and-title-50-issues-when-computer-network-operations-impact-third-countries.

[82] Anmerkungen von Mieke Eoyang, Panel on Offensive Cyber während des Center for Cybersecurity Policy and Law (Regisseur). 8. Oktober 2025. CyberNext DC 2025 [Videoaufzeichnung]. https://www.youtube.com/watch?v=VxtE68RcqXs

[83] United States Government Accountability Office (2022, März). *VERTEIDIGUNGSBESCHAFFUNG: Das Cyber Command muss Kennzahlen zur Bewertung der Kampffähigkeiten entwickeln.* https://www.gao.gov/assets/gao-22-104695.pdf; United States Government Accountability Office (19. November 2020). *Beschaffung von Verteidigungsgütern: Eine gemeinsame Architektur für die Cyberkriegsführung würde von definierten Zielen und Governance profitieren | US GAO.* Abgerufen am 16. März 2025 von https://www.gao.gov/products/gao-21-68 ; Carley Welch. *Cyber Command will Softwarefabriken von Armee und Luftwaffe unter JCWA vereinen, Pläne für neuen PEO.* Breaking Defense, 6. Juni 2024. https://breakingdefense.com/2024/06/cyber-command-wants-to-unify-army-and-air-force-software-factories-under-jcwa-plans-for-new-peo/. Bestätigt durch Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines ehemaligen Regierungs- und aktuellen Branchenteilnehmers, 3. Oktober 2025. 84

Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines ehemaligen Regierungsteilnehmers, 3. Oktober 2025.

[85] Suzanne Smalley. Das *Rotationsproblem des Cyber Command verschärft den Fachkräftemangel angesichts der wachsenden digitalen Bedrohung.* CyberScoop, 18. August 2022. https://cyberscoop.com/military-rotation-norms-challenge-cyber-command/

86Erica Lonergan et al. Aufbau der zukünftigen US-Cyberstreitkräfte. FDD, 9. September 2025. https://www.fdd.org/analysis/2025/09/09/building-the-future-us-cyber-force/

[87] *Diskussion zum Thema Eigenkapital beim FBI, Nutzung von Zero-Day-Angriffen und Richtlinien, Richtlinie und Prozess zum Thema Eigenkapital bei Sicherheitslücken.* FBI, April 24, 2014. https://www.aclu.org/sites/default/files/field_document/zero_days_policy_foia_-_fbi_response.pdf

[88] Sidney Fussell. *Die Spyware, die El Chapos Drogenimperium zu Fall brachte.* The Atlantic, 15. Januar 2019. https://www.theatlantic.com/technology/archive/2019/01/fbi-used-el-chapos-own-spies-against-him/580324/

[89] *Magnet Forensics Part 01 (Final).* (nd). [Datei]. FBI. Abgerufen am 15. Oktober 2025 von https://vault.fbi.gov/magnet-forensics/magnet-forensics-part-01-final

[90] Gaby Del Valle. *Das FBI gelangte innerhalb von nur 40 Minuten in das Telefon des Trump-Rallye-Schützen.* The Verge, 19. Juli 2024. https://www.theverge.com/2024/7/19/24201935/fbi-trump-rally-shooter-phone-thomas-matthew-crooks-cellebrite

[91] Amt für Öffentlichkeitsarbeit des Justizministeriums. *Britischer Staatsbürger im Zusammenhang mit mehreren Cyberangriffen, darunter auch auf kritische Infrastrukturen, angeklagt.* US-Justizministerium, 18. September 2025. https://www.justice.gov/opa/pr/united-kingdom-national-charged-connection-multiple-cyber-attacks-including-critical

[92] DOJ Office of Public Affairs. *Fünf russische GRU-Offiziere und ein Zivilist wegen Verschwörung angeklagt Hack der ukrainischen Regierung.* US-Justizministerium, 5. September 2024. https://www.justice.gov/archives/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government

93In der Angelegenheit der Beschlagnahme aller Gelder von einem Kryptowährungskonto gemäß 18 USC 981, 982 und 28 USC 2461(c), Antrag auf einen Haftbefehl zur Beschlagnahme von Eigentum, das der Einziehung unterliegt. Fall Nr. 24-sz-27, Bezirksgericht der Vereinigten Staaten für den District of Columbia, 21. Juni 2024. https://www.justice.gov/usao-dc/media/1410771/dl?inline

[94] *VEREINIGTE STAATEN VON AMERIKA V. CA. 127.271 BITCOIN („BTC“) VORHER GESPEICHERT AN DEN IN ANHANG A AUFGEFÜHRTEN ADRESSEN FÜR VIRTUELLER WÄHRUNG UND ALLE ERLÖSE SIND DORTHIN ZURÜCKVERFOLGBAR.* Bezirksgericht der Vereinigten Staaten, Östlicher Bezirk von New York. Fall 1:25-cv-05745. 14. Oktober 2025. https://www.justice.gov/usao-edny/media/1416266/dl

[95] Matt Burgess, Andy Greenberg. *Feds beschlagnahmten Bitcoin im Rekordwert von 15 Milliarden Dollar aus mutmaßlichem Betrug Empire.* Wired, 14. Oktober 2025. *https://www.wired.com/story/feds-seize-record-breaking-15-billion-in-bitcoin-from-alleged-scam-empire/*

96Pressemitteilung: USA und Großbritannien ergreifen die bisher umfangreichste Maßnahme gegen cyberkriminelle Netzwerke in Südostasien. US-Finanzministerium, 14. Oktober 2025. https://home.treasury.gov/news/press-releases/sb0278 .

FBI-Bericht zur Internetkriminalität, 2024. FBI-Beschwerdezentrum für Internetkriminalität (IC3). Abgerufen am 7. Oktober 2025 von https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf .

97 USA und Großbritannien ergreifen die bisher umfangreichste Maßnahme gegen cyberkriminelle Netzwerke in Südostasien. (14. Oktober 2025). US-Finanzministerium. https://home.treasury.gov/news/press-releases/sb0278.

98 *VEREINIGTE STAATEN VON AMERIKA V. CA. 127.271 BITCOIN („BTC") VORHER GESPEICHERT AN DEN IN ANHANG A AUFGEFÜHRTEN ADRESSEN FÜR VIRTUELLER WÄHRUNG UND ALLE ERLÖSE SIND DORTHIN ZURÜCKVERFOLGBAR.* Bezirksgericht der Vereinigten Staaten, Östlicher Bezirk von New York. Fall 1:25-cv-05745. 14. Oktober 2025. https://www.justice.gov/usao-edny/media/1416266/dl

999.7.10 Internationale Beschlagnahmungen und Einziehungen. Internal Revenue Service. Abgerufen am 7. Oktober 2025 von https://www.irs.gov/irm/part9/irm_09-007-010

100 *HÄUFIG GESTELLTE FRAGEN ZUR RECHTSHILFE IN STRAFSACHEN.* Büro für internationale Angelegenheiten des US-Justizministeriums (April 2022). https://www.justice.gov/criminal/criminal-oia/file/1498811/dl?inline=

101 Richard Salgado. *Erste Einblicke in das CLOUD Act-Abkommen zwischen den USA und Großbritannien.* Lawfare, 10. März 2025. https://www.lawfaremedia.org/article/first-insights-into-the-us-uk-cloud-act-agreement

102 *Operation Endgame.* Abgerufen am 9. Oktober 2025 von https://operation-endgame.com/

103 Sidney Fussell. *Die Spyware, die El Chapos Drogenimperium zu Fall brachte.* The Atlantic, 15. Januar 2019. https://www.theatlantic.com/technology/archive/2019/01/fbi-used-el-chapos-own-spies-against-him/580324/

104 Darüber hinaus sind nicht alle Partner so freundlich: Als 12 russische Geheimdienstler angeklagt wurden wegen Nach dem Hackerangriff auf das Democratic National Committee im Jahr 2016 deutete Wladimir Putin an, dass das Justizministerium im Rahmen des 1999 zwischen Russland und den USA unterzeichneten Rechtshilfeabkommens um Unterstützung bitten solle. Congressional Research Service. *Vertrag über Rechtshilfe mit der Russischen Föderation: Eine Skizze.* Produktnummer LSB10176, 24. Juli 2018. https://www.congress.gov/crs-product/LSB10176

105 James Landreth, *PE. Durch das Tal des Todes des Verteidigungsministeriums – Die Reise eines datenintensiven Startups.* Defense Acquisition Magazine, Jan.-Feb. 2022. Abgerufen am 15. Oktober 2025 von https://www.dau.edu/library/damag/january-february2022/valley-death

106 Jen Roberts. *Mythische Bestien: Eintauchen in die Tiefen des globalen Spyware-Marktes.* Atlantic Council, 10. September 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/mythical-beasts-diving-into-the-depths-of-the-global-spyware-market/

107 Chris Metinko: *Finanzierung eines Risikokapitalunternehmens im Verteidigungssektor nimmt Fahrt auf.* Crunchbase News, 12. Februar 2025. https://news.crunchbase.com/venture/defense-tech-funding-growth-yir-2024/

108 Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen von aktuellen Risikokapitalgebern und der Industrie Teilnehmer, 3. Oktober 2025.

109 *IQT | Portfolio.* In-Q-Tel. Abgerufen am 7. Oktober 2025 von https://www.iqt.org/portfolio?category=Cyber

110 Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen von aktuellen Risikokapitalgebern und der Industrie Teilnehmer, 3. Oktober 2025.

111 Winnona DeSombre Bernsen. *Crash (Exploit) and Burn: Sicherung der offensiven Cyber-Lieferkette für China im Cyberspace entgegentreten.* Atlantic Council, 25. Juni 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/

112 Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen von aktuellen Risikokapitalgebern und der Industrie Teilnehmer, 3. Oktober 2025.

113 Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen von aktuellen Risikokapitalgebern und der Industrie Teilnehmer, 3. Oktober 2025.

114 Thomas Brewster. *Der von Peter Thiel unterstützte Cyber-Warfare-Anbieter Boldend wird übernommen.* Forbes, 6. August 2024. https://www.forbes.com/sites/thomasbrewster/2024/08/06/boldend-a-peter-thiel-backed-hacking-startup-acquired-by-sixgen/

[115] *Leidos übernimmt Kudu Dynamics und erweitert damit die KI-Fähigkeiten für Cyber-Kämpfer.* Abgerufen 7. Oktober 2025, von https://www.leidos.com/insights/leidos-acquires-kudu-dynamics-advancing-ai- capabilities-cyber-warfighters

[116] Lorenzo Franceschi-Bicchierai. *Der Spyware-Hersteller NSO Group bestätigt die Übernahme durch US-Investoren.* TechCrunch, 10. Oktober 2025. https://techcrunch.com/2025/10/10/spyware-maker-nso-group-confirms- acquisition-by-us-investors/

[117] Andy Greenberg. *Inside Endgame: Ein zweiter Akt für das Blackwater des Hackings.* Forbes, 12. Februar 2024. https://www.forbes.com/sites/andygreenberg/2014/02/12/inside-endgame-a-new-direction-for-the-blackwater-of-hacking/

[118] *CNAS-CEO Nathaniel Fick wird Leiter des Cybersicherheitssoftwareunternehmens Endgame Inc.* CNAS, 7. November 2012. https://www.cnas.org/press/press-release/cnas-ceo-nathaniel-fick-to-lead-cyber-security-software-company-endgame-inc

[119] *Elastic schließt die Übernahme von Endgame ab, einem führenden Anbieter im Bereich Endpoint Protection.* Elastic, 8. Oktober 2019. https://www.elastic.co/en-us/about/press/elastic-completes-the-acquisition-of-endgame-a-leader-in-endpoint-protection

[120] *Elastic schließt die Übernahme von Endgame ab, einem führenden Anbieter im Bereich Endpoint Protection.* Elastic, 8. Oktober 2019. https://www.elastic.co/en-us/about/press/elastic-completes-the-acquisition-of-endgame-a-leader-in-endpoint-protection. *Leidos übernimmt Kudu Dynamics und erweitert damit die KI-Fähigkeiten für Cyber-Kämpfer.* Leidos. Abgerufen am 7. Oktober 2025 von https://www.leidos.com/insights/leidos-acquires-kudu-dynamics-advancing-ai-capabilities-cyber-warfighters .

[121] Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines aktuellen Branchenteilnehmers, 3. Oktober 2025.

[122] Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen aus der aktuellen Industrie und Risikokapital Teilnehmer, 3. Oktober 2025.

[123] Pat Host, *Wie Anduril Innovationen im Bereich der nationalen Sicherheit vorantreibt.* GovCon Wire, 1. Oktober 2025. https://www.govconwire.com/articles/anduril-uav-uuv-lattice-homeland-security

[124] Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen von aktuellen Teilnehmern aus der Industrie und der Regierung, 3. Oktober 2025.

[125] *westonbrown/Cyber-AutoAgent: KI-Agent für autonome Cyberoperationen.* GitHub. Abgerufen am 9. Oktober 2025 von https://github.com/westonbrown/Cyber-AutoAgent

[126] Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen aus der aktuellen Industrie und Risikokapital Teilnehmer, 3. Oktober 2025.

[127] *Justizhandbuch | 9-48.000 – Gesetz gegen Computerbetrug und -missbrauch.* Justizministerium der Vereinigten Staaten, 19. Februar 2025. https://www.justice.gov/jm/jm-9-48000-computer-fraud

[128] *18 US Code § 1030 – Betrug und damit verbundene Aktivitäten im Zusammenhang mit Computern.* LII / Rechtliche Informationen Institut. Abgerufen am 6. Oktober 2025 von https://www.law.cornell.edu/uscode/text/18/1030

[129] Dartmouth ISTS Offensive Cyber Roundtable, Anmerkung eines aktuellen Branchenteilnehmers, 3. Oktober 2025. 130

Justizhandbuch | 9-48.000 – Gesetz gegen Computerbetrug und -missbrauch. Justizministerium der Vereinigten Staaten, 19. Februar 2025. https://www.justice.gov/jm/jm-9-48000-computer-fraud

[131] Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen aktueller Branchenteilnehmer, 3. Oktober 2025.

132Erica D. Borghard, Shawn W. Lonergan. *Was bedeuten die Änderungen der Trump-Administration an PPD-20 für offensive Cyberoperationen der USA?* Council on Foreign Relations. 10. September 2018. https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations

[133] Stacy H. O'Mara. *Zurückhacken oder nicht zurückhacken? Das ist hier die Frage … oder doch nicht?* Center for Cybersecurity Policy and Law, 28. Mai 2025. https://www.centerforcybersecuritypolicy.org/insights-and-research/to-hack-back-or-not-hack-back-that-is-the-question-or-is-it

[134] Clement Lecigne, Maddie Stone. *Aktive nordkoreanische Kampagne gegen Sicherheitsforscher.* Google, 7. September 2023. https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/

[135] Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen aktueller Branchenteilnehmer, 3. Oktober 2025. 136

Büro für Öffentlichkeitsarbeit des Justizministeriums. *Einwohner von New York bekennt sich schuldig, eine geheime Polizeistation der chinesischen Regierung in Lower Manhattan betrieben zu haben.* US-Justizministerium, 18. Dezember 2024. https://www.justice.gov/archives/opa/pr/new-york-resident-pleads-guilty-operating-secret-police-station-chinese-government-lower

137Stephen Smith. *US-Bericht: Berüchtigtes Kartell heuerte Hacker an, um Überwachungskameras und Telefondaten zu nutzen, um FBI-Informanten aufzuspüren und zu töten.* CBS News, 30. Juni 2025. https://www.cbsnews.com/news/sinaloa-cartel-hacker-phone-data-cameras-track-kill-fbi-informants-doj. Bestätigt durch Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen aktueller Branchenteilnehmer, 3. Oktober 2025.

[138] Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen aktueller Branchenteilnehmer, 3. Oktober 2025. 139

Asaf Lubin. WhatsApps juristischer Triumph über die NSO Group. Lawfare, 7. Januar 2025. https://www.lawfaremedia.org/article/unpacking-whatsapp-s-legal-triumph-over-nso-group

[140] *Forschungsbedrohungen: Rechtliche Bedrohungen für Sicherheitsforscher.* Sicherheitsforschungsbedrohungen. Abgerufen 8. Oktober 2025, von http://threats.disclose.io/

141Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines aktuellen Branchenteilnehmers, 3. Oktober 2025.

142Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines aktuellen Branchenteilnehmers, 3. Oktober 2025.

[143] Teilnehmer des Dartmouth-Rundtischgesprächs in der Regierung bestätigten, dass es Generalunternehmern möglicherweise an hochqualifizierten Fachkräften mangelt oder sie Schwierigkeiten haben, diese zu halten, sodass diese beiden Ansätze nicht zu identischen Ergebnissen führen. Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen aktueller Regierungsteilnehmer, 3. Oktober 2025.

[144] Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines Risikokapitalteilnehmers, 3. Oktober 2025. 145

Dartmouth ISTS Offensive Cyber Roundtable, Anmerkungen von Risikokapitalteilnehmern, 3. Oktober 2025.

146T. Dullien. *Weird Machines, Exploitability und Provable Unexploitability.* IEEE Transactions on Emerging Topics in Computing, Bd. 8, Nr. 2, S. 391–403, 1. April–Juni 2020, doi: 10.1109/TETC.2017.2785299. http://www.dullien.net/thomas/weird-machines-exploitability.pdf .

[147] Sergey Bratus. *Technische Perspektive: Wie Exploits die Informatiktheorie beeinflussen.* Mitteilungen der ACM, 22. November 2024. https://cacm.acm.org/research-highlights/technical-perspective-how-exploits-impact-computer-science-theory/

[148] Winnona DeSombre Bernsen. *Crash (Exploit) and Burn: Sicherung der offensiven Cyber-Lieferkette für China im Cyberspace entgegentreten.* Atlantic Council, 25. Juni 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/. Bestätigt durch Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines aktuellen akademischen Teilnehmers, 3. Oktober 2025.

[149] Perri Adams, Dave Aitel, George Perkovich, JD Work. *Verantwortungsvolle Cyber-Offensive.* Lawfare, 2. August 2021. https://www.lawfaremedia.org/article/responsible-cyber-offense

[150] Perri Adams, Dave Aitel, George Perkovich, JD Work. *Verantwortungsvolle Cyber-Offensive.* Lawfare, 2. August 2021. https://www.lawfaremedia.org/article/responsible-cyber-offense

[151] *Verantwortungsvolle Cyber-Macht in der Praxis.* GOV.UK. Abgerufen am 8. Oktober 2025 von https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html. Bestätigt durch Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines aktuellen Teilnehmers der britischen Regierung, 3. Oktober 2025.

[152] *REDSPICE.* Australische Signaldirektion. Abgerufen am 15. Oktober 2025 von https://www.asd.gov.au/about/what-we-do/redspice

[153] *Verantwortungsvolle Cyber-Macht in der Praxis.* GOV.UK. Abgerufen am 8. Oktober 2025 von https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html

[154] Winnona DeSombre Bernsen. *Crash (Exploit) and Burn: Sicherung der offensiven Cyber-Lieferkette für China im Cyberspace entgegentreten.* Atlantic Council, 25. Juni 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/

[155] Matan Mimran. *Die langfristigen Bedrohungen durch die Vault 7-Leaks.* Abgerufen am 8. Oktober 2025 von https://www.cybereason.com/blog/vault-7-leaks-long-term-threats

[156] Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines aktuellen Branchenteilnehmers, 3. Oktober 2025. 157

Anduril stellt den 300. autonomen Überwachungsturm (AST) bereit und verbessert damit die Möglichkeiten zur Grenzsicherheit. Anduril, 26. September 2024. https://www.anduril.com/anduril-deploys-300th-autonomous-surveillance-tower-ast-advancing-capability-for-border-security/

[158] *Wie die Regierung das SBIR-Programm nutzen kann, um Innovationen voranzutreiben.* Anduril, 15. Juli 2021. https://www.anduril.com/how-the-government-can-use-the-sbir-program-to-scale-innovation/

[159] *Programme für Innovation* . Abgerufen am 13. Oktober 2025 von https://www.nsa.gov/business/programs/programs-for-innovation/

[160] Hinweis: Zum Zeitpunkt der Erstellung dieses Dokuments, während der Regierungsschließung am 13. Oktober 2025, sind alle Genehmigungen für das SBIR-Programm abgelaufen. Der Kongress muss sicherstellen, dass die Genehmigung für das SBIR-Programm mit der Verabschiedung des Haushalts erneuert wird .

Themen und Themensuche (SITIS). DOD SBIR-Programm. Abgerufen am 13. Oktober 2025 von https://www.dodsbirsttr.mil/topics-app/

[162] Hossein Siadati, Haadi Jafarian, Sima Jafarikhah. *An welches Konto senden? Evaluation eines LLM-basiertes Scambaiting-System* (Nr. arXiv:2509.08493). arXiv. 10. September 2025. https://doi.org/10.48550/arXiv.2509.08493

[163] Sezaneh Seymour, Brandon Wales. *Partner oder Provokateure? Beteiligung des Privatsektors an offensiven Cyberoperationen.* Lawfare, 16. Juli 2025. https://www.lawfaremedia.org/article/partners-or-provocateurs--private-sector-involvement-in-offensive-cyber-operations

[164] Cyber Lunarium Commission. *CLC Nr. 002: Cyber-Kaperbriefe für Cyberoperationen gegen den IS.* Cyber Lunarium Commission, 9. Juni 2020. https://www.cyberlunarium.org/2020/06/clc-002-cyber-letters-of-marque-for.html

[165] Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines aktuellen Regierungsteilnehmers, 3. Oktober 2025. 166

Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines ehemaligen Regierungsteilnehmers, 3. Oktober 2025. 167

Dartmouth ISTS Offensive Cyber Roundtable, Bemerkung eines ehemaligen Regierungsteilnehmers, 3. Oktober 2025.

168In *der Angelegenheit der Beschlagnahme aller Gelder von einem Kryptowährungskonto gemäß 18 USC 981, 982 und 28 USC 2461(c), Antrag auf einen Haftbefehl zur Beschlagnahme von Eigentum, das der Einziehung unterliegt.* Fall Nr. 24-sz-27, Bezirksgericht der Vereinigten Staaten für den District of Columbia, 21. Juni 2024. https://www.justice.gov/usao-dc/media/1410771/dl?inline

[169] EIDESSTATTLICHE ERKLÄRUNG ZUR UNTERSTÜTZUNG EINES ANTRAGS AUF EINEN BESCHLAGNAHMEBEFEHL. Fall 3:21-mj-70945-LB. US-Bezirksgericht, nördlicher Bezirk von Kalifornien – San Francisco, 7. Juni 2021. https://www.justice.gov/archives/opa/press-release/file/1402056/dl

[170] 18 US Code § 981 – Zivilrechtlicher Verfall. LII / Legal Information Institute. Abgerufen am 16. Oktober 2025 von https://www.law.cornell.edu/uscode/text/18/981

[171] *Ausländer, ausländisches Eigentum und der vierte Verfassungszusatz: United States v. Verdugo-Urquidez, 110 S. Ct. 1056 (1990)* | Amt für Justizprogramme. Abgerufen am 13. Oktober 2025 von https://www.ojp.gov/ncjrs/virtual-library/abstracts/foreigners-foreign-property-and-fourth-amendment-united-states-v

[172] Clement Njoki. *Ethisches Scambaiting: Strategien, Herausforderungen und globale Lösungen verstehen.* GASA, 21. Mai 2024. https://www.gasa.org/post/ethical-scambaiting-understanding-strategies-challenges-and-global-solutions

[173] CBC News. *Infiltrieren von Betrügernetzwerken mit den weltbesten Betrugsbekämpfern | Marktplatz* [Video Aufnahme]. 21. März 2025. https://www.youtube.com/watch?v=MSa7i92o6ho, Dartmouth ISTS

[174] Offensive Cyber Roundtable, Anmerkungen aktueller Branchenteilnehmer, 3. Oktober 2025.

[175] *FBI-Bericht zur Internetkriminalität, 2024.* FBI Internet Crime Complaint Center (IC3). Abgerufen am 7. Oktober. 2025 von https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[176] *Faktenblatt: Präsident Donald J. Trump unterzeichnet GENIUS Act.* Das Weiße Haus, 18. Juli 2025. https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-signs-genius-act-into-law/

[177] *FBI-Bericht zur Internetkriminalität, 2024.* FBI-Beschwerdezentrum für Internetkriminalität (IC3). Abgerufen am 7. Oktober 2025 von https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf .

[178] *SAM.gov.* IRS-Vorschlag zur „Entwicklung von Ausnutzungstechniken gegen Kryptowallets". Abgerufen am 15. Oktober 2025 von https://sam.gov/opp/2b4b9384655e4237862484106c16e581/view

[179] Matt Burgess, Andy Greenberg. *Feds beschlagnahmt Bitcoin im Rekordwert von 15 Milliarden Dollar aus mutmaßlichem Betrugsimperium.* Wired, 14. Oktober 2025. *https://www.wired.com/story/feds-seize-record-breaking-15-Milliarden in Bitcoin aus einem angeblichen Betrugsimperium/*

[180] Chainalysis-Team. *Die Landschaft pfändbarer Krypto-Assets im Jahr 2025.* Chainalysis, 9. Oktober 2025. https://www.chainalysis.com/blog/landscape-of-seizable-crypto-assets-2025/

[181] *FAQ — LazarusBounty.* Bybit. Abgerufen am 13. Oktober 2025 von https://www.bybit.com/en/help-center/article/www.bybit.com/en/help-center/article/FAQ-LazarusBounty

[182] Vicky Ge Huang. *Krypto-Hamsterwahn kühlt nach glühend heißem Sommer ab.* Wall Street Journal, Oktober 1, 2025. https://www.wsj.com/finance/currencies/crypto-stockpiling-craze-cools-after-red-hot-summer- d1b6dce2

183Chainalysis-Team. *Vermögensbeschlagnahme und Kryptowährung: Wie Chainalysis Möglichkeiten für eine selbsttragende Strafverfolgung schafft.* Chainalysis-Blog, 26. März 2025. Abgerufen am 13. Oktober 2025 von https://www.chainalysis.com/blog/cryptocurrency-asset-seizure/

Das Institute for Security Technology Studies (ISTS) wurde im Jahr 2000 am Dartmouth College als nationales Zentrum für Sicherheitsforschung und -entwicklung gegründet. Das Institut führt interdisziplinäre Forschungs- und Entwicklungsprojekte durch, die sich mit den Herausforderungen der Cybersicherheit und der inneren Sicherheit befassen, um die Integrität des Internets, von Computernetzwerken und anderen voneinander abhängigen Informationsinfrastrukturen zu schützen. Das ISTS entwickelt außerdem Technologien zur Bereitstellung der notwendigen Informationen und Werkzeuge, um Gemeinden und Ersthelfer in der sich entwickelnden, komplexen Sicherheitslandschaft zu unterstützen.