Jason Bartlett: Exposing the Financial Footprints of North Korea's Hackers. Washington, D.C.: Center for a New American Security (CNAS), November 2020

Besprochen von **Martin Eduard Debusmann**, LL.M. MPhil MA, Strategic Advisor bei PwC Strategy&, Alumnus der Bundesakademie für Sicherheitspolitik. Zürich, Schweiz, E-Mail: martin.debusmann@pwc.ch

<https://doi.org/10.1515/sirius-2021-3023>

Jason Bartlett, *Research Assistant für Energy, Economics, and Security* am *Center for a New American Security*, nimmt in seiner Studie an die amerikanische Regierung Cyberangriffe Nordkoreas auf die Vereinigten Staaten und ihre Verbündeten in den Fokus. Das Papier ist als *Policy Recommendation* in einem für europäische Verhältnisse deutlich aktionistischem Stil gehalten. Es sei daher besonders hervorgehoben, dass die folgende Zusammenfassung keine Meinung des Rezensenten wiedergibt.

Nordkorea betreibe, so Bartlett, umfassende Cyberverbrechen, u. a. das Umgehen von Sanktionen und globalen Sicherheitsregelungen, digitale Bankraube, Hackerangriffe, betrügerische Banküberweisungen, manipulierte Auszahlungen an Geldautomaten, *Ransomware*-Angriffe mit Lösegeldzahlungen in Kryptowährung und das Hacken der Börsen von Kryptowährungen. Mit diesen Aktionen beabsichtige es, sein illegales Atomwaffenprogramm zu finanzieren. Besonders seit 2020 habe Nordkorea versucht, "internationale Transaktionen von Banken zu manipulieren sowie unautorisierte Auszahlungen an Geldautomaten auszulösen. Im Fokus hätten bisher vor allem Südkorea, Japan und Spanien gestanden. Das *Panel of Experts* des VN-Sicherheitsrats habe 2019 bestätigt, dass Nordkorea versucht habe, zwei Milliarden US Dollar von Auslands-

banken, Finanzinstituten sowie den Börsen für Kryptowährungen zu stehlen.

Das gewählte Vorgehen mittels Cyberoperationen sei zwar sowohl risikoarm als auch kostengünstig, gerade im Verhältnis zu der erwarteten hohen Ausbeute oder zum Ausmaß des verursachten Schadens. Die Finanztransaktionen seien jedoch komplex und Nordkorea bedürfte oft der Unterstützung Dritter wie China, Russland und Indien. Unter anderem der mit diesen Ländern vereinbarte Technologieaustausch, das Angebot der akademischen Ausbildung und die vorsätzliche Blindheit vieler Regulierungsbehörden seien Voraussetzung für Nordkoreas Erfolg. Gerade die Ausbildung von Hackern nehme eine herausragende Rolle ein: Allein im Mai 2020 hätte Nordkorea beispielsweise mindestens 100 Top-Absolventen für seine Cyberaktivitäten anwerben können. Insgesamt seien 6.000 nordkoreanische Cyberagenten weltweit im Einsatz, die in verschiedene Gruppen aufgeteilt seien. Geführt vom Geheimdienst (*Reconnaissance General Bureau, RGB*) und seinem *Bureau 121* gehörten zu den wichtigsten Akteuren demnach die *Lazarus Group* (Netzwerkangriffe und -infiltrationen, *social chaos*), die *Andariel/Andarial Group* (Informationsbeschaffung), die *Bluenoroff Group* (*Financial Cyber Crime*), *APT37* (Cyberspionage) und *APT38* (Attacken auf Banken und Finanzinstitute).

Bartlett gibt einige konkrete Beispiele für nordkoreanische Ausbildungsprogramme und unterstützende Allianzen mit Russland, Indien und China. Als Gegenmaßnahmen schlägt der Autor folgende Maßnahmen vor:

- Die Einrichtung einer auf Nordkorea spezialisierten *Cyber Exchange* analog zur *FinCEN Exchange*, die den Informationsaustausch zwischen amerikanischen Behörden erleichtern solle. Ausländische Behörden könnten ebenfalls einbezogen werden. Das Programm solle innerhalb des *Office of Foreign Assets Control* (OFAC) des Finanzministeriums angesiedelt sein.
- Das amerikanische Justizministerium solle Strafzahlungen gegenüber denjenigen Finanzinstituten aussprechen, die Sicherheitsmaßnahmen (wie sie etwa seitens der *Cybersecurity & Infrastructure Security Agency*, des Finanzministeriums oder der *FAFT Financial Action Task Force* vorgesehen seien) nicht eingeführt hätten und damit Schwachstellen für Angriffe auf das Finanzsystem insgesamt zuließen.
- Die amerikanischen Finanzinstitutionen sollten regelmäßige Gespräche zur Cybersicherheit mit ihren ausländischen Referenzbanken anstrengen, um ihre Transaktionen und die Verwendung des US-Dollars insgesamt zu schützen. Kooperationen mit unsicheren Korrespondenzbanken sollten eingestellt und

alle Verdachtsfälle dem Finanzministerium gemeldet werden. Die amerikanischen Finanzinstitute könnten zu einem solchen Vorgehen motiviert werden, indem nur ein solch konsequentes Handeln sie vor eigenen Strafverfahren schützen könne.

- Das amerikanische Außenministerium solle die Nachverfolgung derjenigen nordkoreanischen Staatsbürger ermöglichen, die in IT- und vergleichbaren Studiengängen in China, Indien, Russland, Weißrussland und Malaysia eingeschrieben sind. Diese Länder seien als wesentliche Schlüsselländer für die Ausbildung nordkoreanischer Cyberagenten im *Army Manual on North Korean Tactics* aufgeführt. Es sollten das *UN Panel of Experts* und die Internationale Atomenergiebehörde sowie NGOs einbezogen werden, die unter anderem relevante Studienpläne analysieren könnten. Das *UN Panel of Experts* habe Vergleichbares bereits bei CSSTEAP (*Centre for Space Science and Technology Education in Asia and the Pacific*) getan.
- Das US-Außenministerium solle zudem die Offenlegung des chinesischen und russischen Austausches mit Nordkorea zu Geheimdienstoperationen und zu deren Einsatz von Schadsoftware anstrengen. Gemeinsam mit amerikanischen Think Tanks, NGOs und abtrünnigen Exilanten sollten die Anzahl und die Aufenthalts- und Wirkungsorte nordkoreanischer Agenten ermittelt werden. Das *UN Panel of Experts* sowie internationale Verbündete sollten anlasskonform eingebunden werden. Die Ergebnisse könnten Gegenstand der Diskussion neuer Sanktionen gegen Nordkorea und deren verbündete Staaten werden, die die VN-Resolution 2397 verletzen.
- Das amerikanische Finanzministerium solle Sanktionen auf alle ausländischen Einheiten und Institutionen ausweiten, die Nordkorea durch Ausbildung, Informationen oder Technologieaustausch unterstützen oder vor deren Cyberverbrechen „die Augen schließen.“ Die USA könnten die *Executive Orders* 13687 und 13694 anwenden, um entsprechende Operationen offenzulegen. Es müsse den ausländischen Agenten durch finanzielle und logistische Hürden erschwert werden, Nordkorea zu unterstützen.

Die Vereinten Nationen sollten, so Bartlett abschließend, andere bereitwillige Staaten anführen, gemeinsam den Kampf gegen Nordkoreas Cyberaktivitäten aufzunehmen. Neben der Erhöhung von technischen Sicherheitsmechanismen und dem zwischenstaatlichen Informationsaustausch solle die Nachverfolgung von gegnerischen Cyberagenten Aufschluss über Nordkoreas Cybereinheiten geben. Eigene Agenten müssten geschult und zum Einsatz gebracht werden.

<https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers>