Aufsatz

Michael Raska*

Nordkoreas Cyber-Krieg Strategie: Kontinuität und Wandel

https://doi.org/10.1515/sirius-2020-2003

Zusammenfassung: Nach Auffassung Pjöngjangs ist die koreanische Halbinsel Schauplatz eines eingefrorenen geopolitischen Konflikts zwischen Großmächten. Die Vereinigten Staaten betreiben dabei eine aus Sicht des nordkoreanischen Regimes „feindselige Politik", die dessen Überleben gefährde und den politischen Gestaltungsraum sowie das wirtschaftliche Entwicklungspotenzial des Landes untergrabe. Während Südkorea und den Vereinigten Staaten vor allem das wachsende Kernwaffenarsenal und die zunehmenden ballistischen Raketenfähigkeiten Nordkoreas Sorgen bereiten, sollte das Bündnis auch der stetigen Weiterentwicklung der nordkoreanischen – offensiven und defensiven – Cyberfähigkeiten mehr Aufmerksamkeit schenken. Nordkorea strebt nach strategischer Überlegenheit, indem es kostengünstige, asymmetrische militärische Fähigkeiten einschließlich Cyberstrategien entwickelt, um Informationen zu sammeln, seine Rivalen unter Druck zu setzen, andere finanziell zu erpressen und auf anderem Wege Einfluss in einer Weise auszuüben, gegen die herkömmliche Abschreckungs- und militärische Gegenmaßnahmen wirkungslos sind. Seoul und Washington benötigen eine umfassende militärische Einsatzstrategie gegen das gesamte Spektrum potenzieller nordkoreanischer Provokationen, während europäische Staaten ihre Cybersicherheitsstrategien verstärken müssen, um die zunehmenden globalen Cyberoperationen Nordkoreas verlässlich aufzuspüren und abzuwehren.

Schlüsselbegriffe: Nordkorea, Cyberkrieg, Cyberkriminalität, hybride Kriegsführung

Abstract: Pyongyang sees the Korean Peninsula as entrenched in a geopolitical deadlock among great powers, with the United States continuing to employ what the North Korean regime sees as a "hostile policy" detrimental to its survival, its ability to shape relevant events, and the country's political and economic development. While the core security concerns of South Korea and the United States are North Korea's growing nuclear weapons and ballistic missile capabilities, the alliance must increasingly also prioritize the continuous development of North Korea's cyber capabilities, both offensive and defensive. North Korea aims to gain strategic advantage by pursuing cost-effective, asymmetric military capabilities, including cyber strategies, to gather intelligence, coerce its rivals, financially extort others, and otherwise exert influence in ways that are resistant to traditional deterrence and defense countermeasures. Seoul and Washington need a full-spectrum military readiness posture against the full range of potential North Korean provocations, while European democracies need to strengthen their cyber readiness posture to effectively track and counter North Korea's evolving global cyber operations.

Keywords: North Korea, Cyberwar, Cybercrime, hybrid warfare

***Kontakt: Dr. Michael Raska**, Assistant Professor an der S. Rajaratnam School of International Studies, Nanyang Technological University, Singapur, E-Mail: ismraska@ntu.edu.sg

1 Einleitung

Seit 2009 haben sich die nordkoreanischen Cyberoperationen, die entsprechenden Organisationsstrukturen und Fähigkeiten ständig weiterentwickelt; dabei kommen unterschiedlichste Taktiken, Techniken und Vorgehensweisen zum Einsatz. Das schließt bestimmte Formen der Cyberspionage und Distributed-Denial-of-Service (DdoS)-Angriffe auf ausgewählte politische und sozioökonomische Ziele in Südkorea ebenso ein wie cybergestützte Informations-, wirtschaftliche und politische Kriegführung weltweit. Tatsächlich wird die wirtschaftliche und politische Kriegführung seit 2014 zunehmend zu einem Schwerpunkt der nordkoreanischen Cyberoperationen; nordkoreanische Cybereinheiten und staatlich finanzierte Hackergruppen versuchen internationale Sanktionen zu unterlaufen und gleichzeitig Ressourcen zu beschaffen, die Nordkorea für seine wirtschaftliche und technologische Entwicklung benötigt.

Nordkoreanische Hacker, die überwiegend vom Ausland aus operieren, haben betrügerische Cyberoperatio-

nen durchgeführt, um Sanktionen zu umgehen und sich Zugang zum internationalen Finanzsystem zu verschaffen, und sie haben mit illegalen Methoden Geldüberweisungen von Finanzinstituten, SWIFT-Bankennetzwerken und Kryptowährungsbörsen auf der ganzen Welt erzwungen.[1] Gleichzeitig ist Nordkorea in der Lage gewesen, seine kritische Infrastruktur vor potenziellen Vergeltungsmaßnahmen zu schützen; es hat seinen Zugang, seine Abhängigkeiten und Angreifbarkeiten über das Internet und andere Kommunikationsnetze dadurch begrenzt, dass es vor allem die chinesische Internetinfrastruktur nutzt. Ergänzt wurde dies in jüngster Zeit durch eine zweite Internetverbindung mit russischen Netzwerken und durch die Entsendung von Hackern in ausgewählte Länder wie Indien, Nepal, Kenia, Mosambik und Indonesien.[2]

Die Cyberoperationen Nordkoreas sind daher im 21. Jahrhundert im Grunde zu „Massenwirksamkeitswaffen" geworden, die zusammen mit den Massenvernichtungswaffen in seinem Arsenal Instrumente einer einheitlichen asymmetrischen politischen Strategie sind, die darauf abzielt, die Vereinigten Staaten und die internationale Gemeinschaft insgesamt durch Druck dazu bringen, die vom Obersten Führer Kim Jong-un vertretene Interpretation der Souveränität und Sicherheit Nordkoreas als legitim anzuerkennen. So hat Kim dem Vernehmen nach im Jahr 2013 erklärt: „Die Fähigkeit zum Cyberkrieg ist zusammen mit Kernwaffen und Raketen ein ‚Allzweckschwert', das sicherstellt, dass unser Militär jederzeit zuschlagen kann."[3]

Bevor wir mit der Analyse beginnen, ein einschränkender Hinweis: Die Bewertung der nordkoreanischen Cyberoperationen und der ihnen zugrunde liegenden strategischen Überlegungen ist eine anspruchsvolle Aufgabe, nicht nur, weil die Zurechnung (einer Operation zu Nordkorea) immer wieder strittig ist, sondern auch wegen der Abschottung des Landes und seiner totalitären Staats- und Gesellschaftsordnung. Entsprechend sind die verfügbaren Daten aus offenen Quellen im Wesentlichen beschränkt auf Berichte über Cyberbedrohungen (Threat Intelligence) und Studien globaler Cybersicherheitsfirmen, ausgewählte Stellungnahmen und Publikationen der US-amerikanischen und südkoreanischen Regierung, ausgewählte nordkoreanische Überläufer mit partiellen Kenntnissen über die nordkoreanischen Cyberaktivitäten, Sekundärliteratur wie etwa Berichte von Denkfabriken und Fachaufsätze und schließlich Hinweise in nordkoreanischen Zeitungen und anderen Medien. Die Datenquellen sind allerdings nicht immer verlässlich und die Aussagekraft der Daten unter Umständen beschränkt; dies liegt unter anderem an tendenziösen Informationen durch Behörden, (verdeckten) politischen Agenden, der Tatsache, dass Daten veraltet sind und dass es Schwachstellen bei der Nachrichtengewinnung gibt.

Divergierende frühere Einschätzungen haben eine anhaltende Debatte über die Richtung, die Eigenart, die Fähigkeiten und den strategischen Stellenwert der nordkoreanischen Cyberoperationen ausgelöst. Einerseits behaupten Skeptiker, dass die Fähigkeit Nordkoreas, den Cyberspace für politische Zwecke zu nutzen, insbesondere auf strategischer Ebene erheblichen Beschränkungen unterliege. Dieser Sichtweise zufolge stärkten die Cyberoperationen allein nicht die nordkoreanischen Fähigkeiten zur Zwangsausübung oder Abschreckung – bislang hätten diese Fähigkeiten noch keine Regierung dazu veranlasst, einzulenken oder ihren Kurs zu ändern, und Pjöngjang habe daraus auch keine nennenswerten politischen, militärischen oder finanziellen Vorteile im Einklang mit seinen wichtigsten strategischen Zielen gezogen.

Folglich – so die Vertreter dieser Sichtweise – verschafften die Cyberfähigkeiten Pjöngjang auch keine erheblichen strategischen Vorteile bezüglich der Erreichung politischer Ziele, und sie seien auch nicht ausreichend, um die fortgeschrittenen Vergeltungsfähigkeiten der USA oder eines anderen Staates zu schwächen und so das Überleben des Regimes sicherzustellen.[4]

Nach der entgegengesetzten Auffassung sind die nordkoreanischen Cyberfähigkeiten, hauptsächlich unter dem Druck strategischer Notwendigkeiten, allmählich immer umfangreicher und komplexer geworden; sie hätten dem Regime in einem feindlichen strategischen Umfeld Handlungsmacht und -freiheit gegeben. Gemäß dieser Sichtweise haben die vielfältigen Cyberoperationen und Operationen zur Informationsgewinnung Pjöngjang relativ

1 Vereinte Nationen 2019, 48–51.

2 Priscilla Moriuchi: North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny, *Recorded Future Blog*, April 25, 2018; https://www.recordedfuture.com/north-korea-internet-behavior/.

3 Hyungsoo Kim, Kim Jong-Un Says 'Cyber Warfare Is an All-Powerful Tool,' Utilizes It as One of Three Major Means of Warfare, *Joongang Ilbo*, 5. November 2013; David Sanger/David Kirkpatrick/Nicole Perlroth: The World Once Laughed at North Korean Cyberpower. No More, *New York Times*, 15. Oktober 2017.

4 Ryan C. Maness/Brandon Valeriano/Benjamin Jensen: North Korea's Offensive Cyber Program Might Be Good, But Is it Effective?, *Blogpost at Council on Foreign Relations, Digital and Cyberspace Policy Program*, 25. Oktober 2017; https://www.cfr.org/blog/north-koreas-offensive-cyber-program-might-be-good-it-effective; James Lewis: North Korea and Cyber Catastrophe—Don't Hold Your Breath, *38 North Blog*, 12. Januar 2018; https://www.38north.org/2018/01/jalewis011218/.

kostengünstige asymmetrische Optionen zur Machtdemonstration ohne sichtbares militärisches Engagement an die Hand gegeben; mit den auf diese Weise beschafften Hunderten von Millionen Dollar seien das Regime und seine Kernwaffen- sowie ballistische Raketenprogramme unterstützt worden, und sie hätten Pjöngjang letztlich auch in die Lage versetzt, unter einem Schleier glaubhafter Abstreitbarkeit strengere Wirtschaftssanktionen erfolgreich zu unterlaufen.[5]

Nordkoreanische Hackergruppen sind tatsächlich in der Lage gewesen, eine breite Palette von Instrumenten und asymmetrischen Methoden zu entwickeln, mit denen sie nationale Ziele verfolgen. So weisen die nordkoreanischen Cyberoperationen mindestens drei besondere Merkmale auf. Erstens zeichnen sich die Cybereinheiten und Hackergruppen durch bemerkenswert breitgefächerte Fähigkeiten und Erfahrungen aus: von gering- bis hochqualifizierten Hackern; und diese Bandbreite hat es noch schwieriger gemacht, ihre Leistungsfähigkeit ausschließlich anhand solcher Kriterien zu messen. Gleichzeitig arbeiten nordkoreanische Hackergruppen von unterschiedlichsten geografischen Standorten aus, und zwar je nach ihren spezifischen Cyberaufträgen entweder unabhängig voneinander oder in enger gegenseitiger Unterstützung. Diese reichen von Cyberspionage zur Nachrichtengewinnung, Informationsmanipulation und politischer Kriegführung bis zu offensiven und defensiven militärischen Cyberoperationen, elektronischer Kriegführung und verdeckter finanzieller Erpressung. Von daher wurde die Trennlinie zwischen einfachen und komplexen nordkoreanischen Operationen im Cyberspace immer wieder verwischt; Nordkorea kann nicht staatliche Akteure als Stellvertreter einsetzen, kostengünstige Standardwerkzeuge, die frei verfügbar sind, nutzen, bekannte Schwachstellen ausnutzen und Techniken wie etwa Denial-of-Service-Angriffe anwenden.

Gleichzeitig kann Nordkorea ressourcen- und aufklärungsintensive Operationen, bei denen Schwachstellen in Systemen aufgedeckt werden, durchführen (sogenannte Zero-Day-Exploits – sofortige Angriffe nach Erkennen der Sicherheitslücke) und Strategien des Abstreitens, der Sabotage, der Zerstörung beziehungsweise der Subversion von Informations- oder physischer Infrastruktur anwenden. Solche – taktischen oder strategischen – Operationen können kurz oder lange dauern.

Die Cyberstrategie und -taktik Nordkoreas ist Ausdruck eines „ganzheitlichen Konzepts der Informationskriegführung, das sämtliche Aspekte der Beeinflussung von Information, wie elektronische Kriegführung, Cyberkriegführung und psychologische Operationen berücksichtigt."[6] Langfristig werden die konvergierenden Cyber-, Nuklear- und konventionellen Strategien Nordkoreas das Bündnis zwischen den USA und Nordkorea vor neue Herausforderungen stellen.

2 Die Cybereinheiten Nordkoreas und ihre Organisationsstruktur

Ein kurzer Blick auf die Ursprünge der nordkoreanischen Cyberoperationen ist ein nützlicher Ausgangspunkt. Das Interesse des Landes an der Cyberkriegführung begann Mitte der 1990er-Jahre, als die Koreanische Volksarmee (KVA) die von der chinesischen Volksbefreiungsarmee (VBA) formulierten Konzepte der „elektronischen nachrichtendienstlichen Kampfführung" studierte und aus der elektronischen Kriegführung und den Cyberoperationen der USA während des Ersten Golfkriegs und des NATO-Einsatzes auf dem Balkan eigene strategische Schlussfolgerungen zog.[7] Im Jahr 1995 wies der damalige Oberste Führer Kim Jong Il den Generalstab der KVA an, Fähigkeiten zur „Informationskriegführung" zu entwickeln.[8] Im September 1998 gründete Nordkorea die Einheit 121 innerhalb der Stabsabteilung Aufklärung der KVA, eine Einheit mit anfänglich wohl zwischen 500 und 1.000 Mitgliedern, die mit der Erforschung und Entwicklung von Cyberangriffstechniken, Verschlüsselungsverfahren und Software-Engineering betraut wurde. Außerdem vernetzten sie sich bei Informatik-Lehrgängen in China und Russland mit dortigen Fachleuten. Laut den Aussagen der beiden nordkoreanischen Cybersicherheitsexperten und Überläufer Kim Heung Kwang und Jang Se Yul bereiteten sie darüber hinaus auch vom Ausland aus Cyberoperationen vor.[9] Die meisten Kader der Einheit 121 wurden aus den Absolventen der führenden Technischen Hochschulen Nordkoreas ausgewählt, wie etwa der *Pyongyang University of Automation* (das frühere *Mirim College*), dem *Amrokgang College of Military Engineering*, der *National Defense University* und

5 Sanger/Kirkpatrick/Perlroth: The World Once Laughed at North Korean Cyberpower. No More, *op cit*.

6 Jun/LaFoy/Sohn 2015, 51.

7 Pinkston 2016.

8 Pinkston 2016, 60.

9 Sangwon Yoon: North Korea Recruits Hackers at School, Aljazeera News, 21. Juni 2011.

der *Pyongyang Computer Technology University*.[10] Damals waren ein Großteil der nordkoreanischen Computer-Infrastruktur und viele der damit verbundenen Einrichtungen lediglich in Ansätzen vorhanden; das Gleiche gilt in den frühen Phasen für einen Großteil der nordkoreanischen Cyberkriegsführungsprogramme, die mit einfachen Cyberangriffstechniken und Schadprogrammen der ersten Generation experimentierten. Im Jahr 2009 gelangte der *U.S. National Intelligence Estimate* zu der Einschätzung, die Cyberfähigkeiten Nordkoreas stellten ebenso wie seine Langstreckenraketenprogramme noch auf Jahre hinaus keine ernsthafte Bedrohung dar.[11]

Im selben Jahr legte Nordkorea all seine Nachrichten- und inneren Sicherheitsdienste zusammen und unterstellte sie zunächst unmittelbar dem Nationalen Verteidigungsausschuss, um die Herrschaft von Kim Jong-un als Nachfolger von Kim Jong Il zu festigen. Nachrichtendienstliche Organisationen und verschiedene Cyberabteilungen und -dienststellen der Koreanischen Arbeiterpartei, der Hauptabteilung für Operationen und des Büros 35 (Auslandsoperationen) sowie das militärnachrichtendienstliche Amt für Aufklärung der Koreanischen Volksarmee wurden unter dem Dach des neu geschaffenen Amts für Allgemeine Aufklärung (RGB) zusammengeführt.[12] Das Amt für Allgemeine Aufklärung wurde zum wichtigsten nordkoreanischen Auslandsnachrichtendienst sowie zur Zentralstelle für Spezial- und Cyberoperationen.[13] Das (zwischen 2009 und 2016) von General Kim Yong Chol geleitete Amt für Allgemeine Aufklärung (RGB) integrierte die Einheit 121, stockte sein Personal auf 3.000 Mitarbeiter auf und wurde zu einer Hauptverwaltung aufgewertet, die auch Büro 121 genannt wird – „Büro zur Cyberkriegführung".[14]

Auch wenn die genaue Organisationsstruktur der Cybereinheiten des RGB durch Geheimhaltung, verschiedene Decknamen und interne Restrukturierungen im Lauf der Jahre verschleiert wurde, deuten Hinweise in frei zugänglichen Publikationen darauf hin, dass Büro 121 die Aufsicht hat über Einheit 91, Einheit 180 und Lab 110, die wichtigsten cyber-bezogenen Komponenten des RGB und seiner sechs Abteilungen (Operationen, Aufklärung, Nachrichtengewinnung im Ausland, innerkoreanischer Dialog, Technische und Rückwärtige Dienste).[15] So umfasst die Cybereinheit des RGB, das Büro 121, wahrscheinlich insbesondere offensive und defensive Untereinheiten und Teams für die cyber-gestützte Nachrichtengewinnung und Cyberangriffe, die nach Zuständigkeiten, Kompetenzen und Aufgabenzuweisung organisiert werden: das Stammauswertungsteam, das Team für Angriffsoperationen, das Team für Dechiffrierung, das Entwicklungsteam, das Inspektionsteam, das Team für Netzwerkanalyse und das Team für Angriffsplanung.[16] Die hauptsächlichen Aufgaben der Einheit sind wahrscheinlich offensive und defensive Cyberoperationen einschließlich Angriffen auf kritische Informationsinfrastruktur – Kommunikationsverbindungen, Verkehrswege, Stromnetze und Flugsicherungssysteme in „unfreundlichen" Staaten – hauptsächlich in den Vereinigten Staaten und Südkorea. Zugleich führt das Büro 121 Cyberspionage gegen Behörden, das Militär, die Rüstungsindustrie und die Medien anderer Zielländer durch.[17]

Unterstützt wird das Büro 121 bei seinen Cyberoperationen wahrscheinlich hauptsächlich vom Forschungslabor für Computertechnologie des RGB – Lab 110; es wird angenommen, dass Lab 110 Software entwickelt, technische Aufklärung leistet, Computernetze infiltriert, durch Hacking Nachrichten gewinnt und Viren in angegriffene Netzwerke einschleust.[18] Auch wenn die genaue operative Beziehung und Zusammenarbeit zwischen Büro 121 und Lab 110 unbekannt ist, analysiert Lab 110 dem Vernehmen nach technologische Konfigurationen und Verhaltensmuster von Zielen und entwickelt dann maßgeschneiderte Software und Schadprogramme, die Büro 121 bei Cyberangriffen verwendet.[19]

Im Juni 2018 hat das US-Justizministerium gegen einen Hacker Anklage erhoben, der mutmaßlich im Auftrag der nordkoreanischen Regierung handelte und an einer Reihe größerer Cyberangriffe beteiligt gewesen sein sollte, u. a. an der Attacke auf Sony Pictures Entertainment und bei dem Einsatz des WannaCry-Erpressungstrojaners, der Hunderttausende von Rechnern in 150 Ländern infizierte und zur Schließung von Dutzenden von Notaufnahmen in britischen Krankenhäusern führte.[20] In der Klage-

10 Ibid.; s. a. Brian McWilliams: North Korea's School for Hackers, Wired Magazine, 6. Februar 2003; https://www.wired.com/2003/06/north-koreas-school-for-hackers/.

11 Sanger/Kirkpatrick/Perlroth: The World Once Laughed at North Korean Cyberpower, op.cit.

12 Bermudez 2010.

13 Jun/LaFoy/Sohn 2015, 51.

14 Sangwon Yoon: North Korea Recruits Hackers at School, op. cit.

15 Bermudez 2010, Bermudez 2016.

16 Lee 2017, 22.

17 Jiro Yoshino: North Korea's Cybertroops Span the Globe in Quest for Cash, Nikkei Asian Review, 15. März 2018; https://asia.nikkei.com/Politics/International-relations/North-Korea-s-cybertroops-span-the-globe-in-quest-for-cash.

18 Tosi 2017, 26.

19 Lee 2017, 22.

20 Hamish Mcdonald: Fog of Cyberwar Spurs Virtual Arms Race On Korean Peninsula, *Nikkei Asian Review*, 22. Mai 2017.

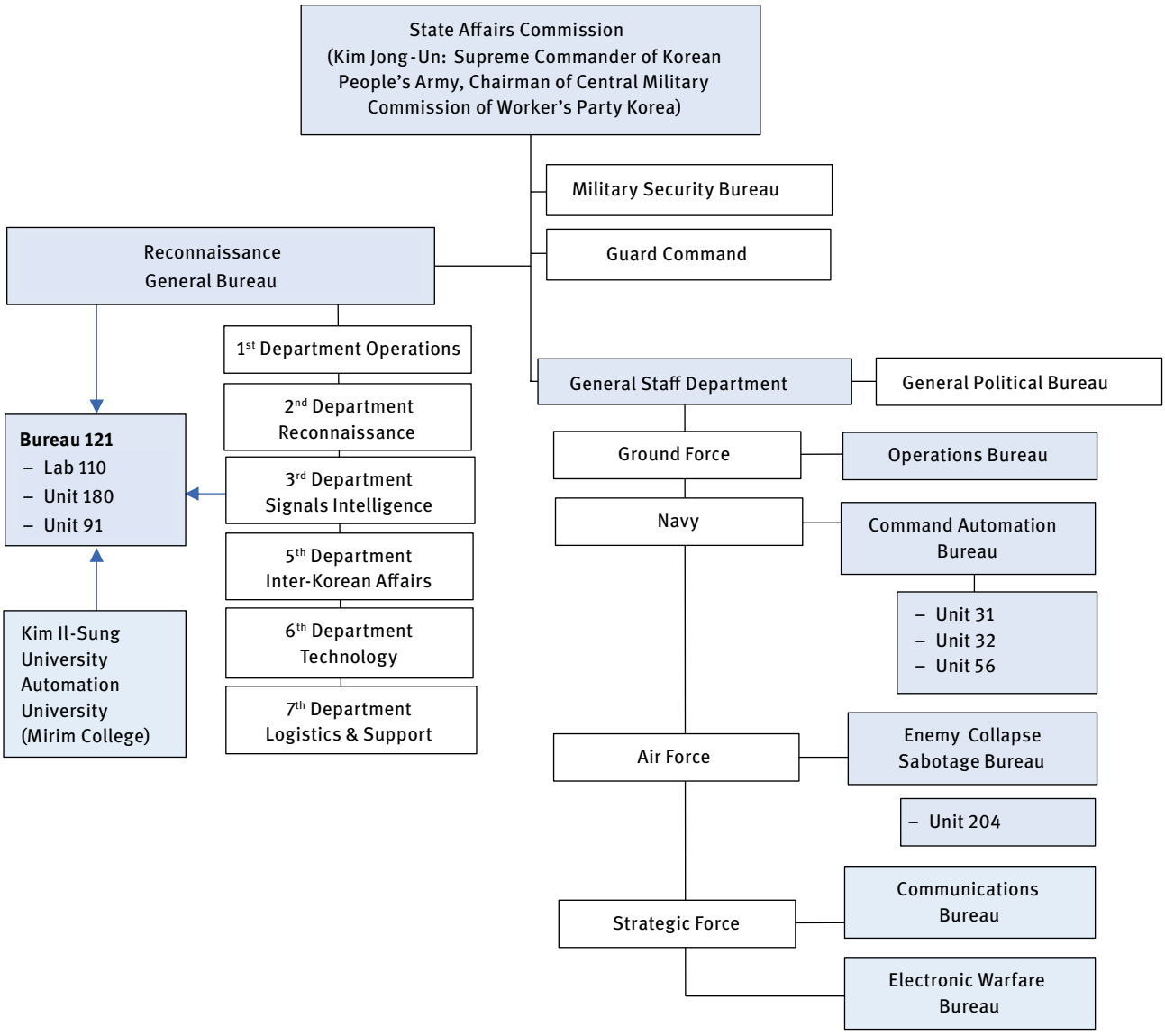


Abb. 1: Die nordkoreanischen Cyberorganisationen im Amt für Allgemeine Aufklärung und im Generalstab
Quelle: Autor; nach dem ROK Defense White Paper 2012; vgl. auch Boo et al. 2013, S. 94; Boo 2017; Jun/LaFo/Sohn 2015; Kong/Lim/Kim 2019; Sang-ho Song: North Korea Bolsters Cyberwarfare Capabilities, *Korea Herald,* 27. Juli 2014, http://www.koreaherald.com/view.php?ud=20140727000135

schrift wird Park Jin Hyuok als ein Mitarbeiter von Lab 110 bezeichnet, der für „eine weitreichende, sich über mehrere Jahre hinziehende Verschwörung [verantwortlich ist], mit dem Ziel, sich unbefugt Zugriff auf Computer zu verschaffen und mit Hilfe von Mitverschwörern, die im Auftrag der Regierung der Demokratischen Volksrepublik Korea handelten, Überweisungsbetrug zu begehen, während sie sich in Nordkorea und in China aufhielten [...] Die Verschwörung richtete sich gegen Computer, die Unterhaltungsfirmen, Finanzinstituten, Rüstungsunternehmen und anderen gehörten, und die Taten geschahen in der Absicht, Schaden anzurichten, Informationen zu gewinnen, Geld zu stehlen und anderes mehr."[21]

Im Jahr 2013 hat das RGB angeblich auf Befehl von Kim Jong-un Einheit 180 geschaffen, die laut Interviews mit Kim Heung-kwang aus etwa 500 Mitarbeitern von Büro 121 besteht und ausdrücklich den Auftrag erhalten haben soll,

21 United States District Court for the Central District of California: Criminal Complaint: United States of America v. Park Jin Hyok, Case No. MJ18-1479, 8. Juni 2018, 3.

internationale Finanzinstitute zu hacken, um Devisen zur Finanzierung des nordkoreanischen Atom- und Langstreckenraketenprogramms zu beschaffen und in kommerzieller Software, die in Japan und China entwickelt wird, Hintertüren für Schadprogramme zu installieren.[22]

In den Jahren 2014–15 soll Nordkorea seine Cyberabteilungen reorganisiert haben – Einheit 180 sollte sich demnach auf Kryptowährungsbörsen spezialisieren. So erklärte der südkoreanische Nachrichtendienst NIS im Januar 2018, der Diebstahl der digitalen Kryptowährung NEM im Wert von 530 Millionen Dollar bei dem Tokioter Börsenbetreiber *Coincheck* sei wahrscheinlich von Einheit 180 verübt worden.[23] Unterdessen dehnte Büro 121 seine Cyberoperationen über Südkorea hinaus aus; Ziel der Angriffe waren ausländische Infrastruktureinrichtungen wie Verkehrsnetze, Telekommunikation, Stromnetze, Kraftwerke und Flugsicherungssysteme.[24] Die Reorganisation der Cyberaktivitäten in den Jahren 2014–2015 erstreckte sich auch auf die elitäre Einheit 91, die ursprünglich den Auftrag hatte, Cyberspionage-Operationen gegen südkoreanische Behörden, Unternehmen und Privatpersonen durchzuführen[25], aber seit 2014/15 damit begonnen hat, schwerpunktmäßig „hochmoderne Technologien, die für das Atomwaffen- und Langstreckenraketenprogramm benötigt werden, von Industrieländern zu erwerben.[26] Im Jahr 2016 wurden sämtliche Cybereinheiten des RGB direkt der Kommission für Staatsangelegenheiten (KSA) unterstellt, die als oberstes politisches Entscheidungsorgan und Machtzentrum der Regierung der Volksrepublik Korea an die Stelle der Nationalen Verteidigungskommission trat.[27]

Neben den Cybereinheiten und -operationen unter Führung des RGB spielen auch die militärischen Cyberelemente der Koreanischen Volksarmee (KVA) und ihres Generalstabs, die für die Integration von Cyberfähigkeiten in konventionelle militärische Operationen verantwortlich sind, eine wichtige Rolle. Die Cyberkriegsstrategie der KVA lehnt sich offenbar eng an die Konzepte der Chinesischen Volksbefreiungsarmee in Bezug auf Elektronische nachrichtendienstliche Kampfführung (EKF), Kriegführung in Computernetzwerken (KCN), psychologische Kriegsführung, militärische Täuschung und Informationskriegführung (IK) an.[28] Generalstabsabteilungen wie die Abteilung für Elektronische Kriegführung und die Abteilung für Feindsabotage (Einheit 204) wurden angeblich mit verschiedenen Maßnahmen der elektronischen, Informations- und psychologischen Kriegsführung beauftragt, die die Effektivität von Cyberoperationen erhöhen sollen, um gemeinsame konventionelle Militäroperationen der Republik Korea und der USA zu stören.[29] Im Vorfeld und während eines Krieges würden integrierte Cyberoperationen der KVA wahrscheinlich als ein asymmetrisches Mittel eingesetzt, um verschiedene Aktionen wie Drohnenangriffe, Operationen von Spezialkräften und Angriffe mit ballistischen Raketen zu unterstützen, die gemeinsamen Führungseinrichtungen der US- und südkoreanischen Streitkräfte zu sabotieren und somit die Unterlegenheit Nordkoreas auf dem Gebiet der konventionellen Militärtechnologie auszugleichen.[30]

Die Einheiten für Cyberkriegführung der KVA sind in die Abteilung „Kommando-Automatisierung" eingebettet: Einheit 31 – zuständig für die Entwicklung von Schadprogrammen; Einheit 32 – zuständig für die Entwicklung militärisch nutzbarer Software und Einheit 56 – zuständig für die Entwicklung von Software für militärische Truppenführung.[31] Diese Einheiten verfügen wahrscheinlich auch über Software-Engineering/Entwicklungsteams, die für die Entwicklung von Werkzeugen und Fähigkeiten zuständig sind, die wahrscheinlich auch von den operativen Abteilungen innerhalb des RGB eingesetzt werden.

Im Jahr 2016 hat der nordkoreanische Generalstab auch eine neue Abteilung für Führung, Kommunikation, Computer und Aufklärung (C4I) im Militär eingerichtet, die an die Stelle des aufgelösten Büros für Kommando-Information getreten ist.[32] Wahrscheinlich soll die neue C4I-Abteilung die Integration offensiver Cyberfähigkeiten in konventionellen Operationen beschleunigen – das heißt, kritische Infrastruktur ins Visier nehmen und, was noch wichtiger ist, die defensiven Cyberfähigkeiten der Führungssysteme der KVA verbessern. Diese wurden angeblich durch das streng geheime militärische Programm der USA zur Ausschaltung nordkoreanischer ballistischer Raketen vor dem Start (*left of launch*) durch Cyberkrieg-

22 Ju-min Park/James Pearson: Exclusive: North Korea's Unit 180, the Cyber Warfare Cell that Worries the West, *Reuters,* 21. Mai 2017.
23 Cynthia Kim: South Korean Intelligence says N. Korean Hackers Possibly behind Coincheck Heist – Sources, *Reuters,* 6. Februar 2018.
24 Steve Miller: Where Did North Korea's Cyber Army Come From?, *Voice of America,* 20. November 2018.
25 Charlie Campbell: Why We Shouldn't Be Surprised If North Korea Launched the WannaCry Ransomware Cyberattack, Time, 17. Mai 2017.
26 Steve Miller: Where Did North Korea's Cyber Army Come From?, op. cit.
27 National Defense Commission (Defunct): NK Leadership Watch website, https://nkleadershipwatch.wordpress.com/dprk-security-apparatus/national-defense-commission.
28 Mansourov 2014.
29 Jun/LaFoy/Sohn 2015, 51.
30 TRADOC NK tactics.
31 Jun/LaFoy/Sohn 2015, 47.
32 Lee 2017, 23.

führung, Energiewaffen und elektronische Angriffe kompromittiert.[33] Als Gegenmaßnahme entwickelt Nordkorea angeblich eine Quantenverschlüsselungstechnologie, um auf diese Weise eine hochgesicherte Verbindung für die Befehlskommunikation zwischen Pjöngjang und wichtigen Raketenabschussbasen wie Wonson, Tonghae und Sohae aufzubauen.[34]

3 Cyberaktivitätscluster in Nordkorea

Ausgehend von Taktiken, Techniken und Vorgehensweisen (*tactics, techniques, and procedures – TTPs*) werden die nordkoreanischen Cybergruppen aus externer Perspektive mit einem hohen Maß an Übereinstimmung klassifiziert – einige Quellen fassen die Cybereinheiten des RGB in ihrer Gesamtheit unter dem Oberbegriff *Lazarus-Gruppe* zusammen und machen diese für sämtliche Nordkorea zugeschriebenen Aktivitäten verantwortlich, während andere nordkoreanische Cluster bzw. Gruppen wie *Bluenoroff, APT37 (Reaper)* und *APT38* getrennt voneinander betrachten. Andere schreiben bestimmte Aktivitäten, die mit diesen Gruppennamen in Verbindung gebracht werden, der Lazarus-Gruppe des RGB zu.[35] Die US-Regierung bezeichnet sämtliche „bösartigen" – in Schädigungsabsicht betriebenen – Cyberaktivitäten der nordkoreanischen Regierung als HIDDEN COBRA.[36] Auf der Basis von frei verfügbaren Bedrohungsanalyseberichten von Behörden und privaten Cybersicherheitsfirmen kann man jedoch zu der Einschätzung gelangen, dass es unter dem Dach des RGB eine Reihe von Untergruppen gibt, die aufgrund ihrer besonderen TTPs nicht der Lazarus-Gruppe zugeordnet werden sollten. Diese Besonderheiten werden in Tabelle 2 berücksichtigt.

Laut einer aktuellen Analyse durch McAfee Labs von Schadprogrammen, die Nordkorea zugeschrieben werden, „verfügen die Nordkoreaner über Gruppen mit unterschiedlichen Fähigkeiten und Werkzeugen, die jeweils gezielte Cyberoperationen ausführen, während sie auch parallel arbeiten, wenn große Kampagnen eine Kombination von Fähigkeiten und Tools erfordern."[37] So haben beispielsweise APT 37 (Reaper), Kimsuky und Sun Team jeweils unterschiedliche TTPs, die auf politische Cyberspionage zugeschnitten sind, während sich die mit Lazarus assoziierten Gruppen Andariel und APT 38 (Bluenoroff) auf finanzielle Erpressung und Cyberkriminalität konzentrieren. Mit den zunehmenden Möglichkeiten und der steigenden Komplexität von TTPs haben die nordkoreanischen Cybereinheiten jedoch im Zuge ihrer Erfahrungen und im Zuge der bei Angriffen auf verschiedene Ziele gewonnenen Erkenntnisse nach und nach ihre Ressourcen, Aktiva, Malware-Arsenale und Programmierfähigkeiten erweitert. Sie profitierten auch von der Zusammenarbeit bei verschiedenen Angriffskampagnen, bei denen sie gemeinsam Netzwerkinfrastruktur nutzten und Schadprogramme kontinuierlich weiterentwickelten, um nicht entdeckt zu werden.

Diese Dinge sind seit 2007 bekannt. Damals begannen globale Cybersicherheitsfirmen, staatliche nordkoreanische Hackergruppen öffentlich zu identifizieren und ihre Aktivitäten systematisch zu erfassen,[38] und mehrere großangelegte Cyberangriffe wurden Nordkorea zugeschrieben. Ausgewählte nordkoreanische Hackergruppen gehen ihren Aktivitäten von Standorten in China, Russland, Südostasien und auch von Europa aus nach; sie agieren unabhängig voneinander, unterstützen sich aber auch gegenseitig, wenn ihre konkreten Cyberaufträge dies erfordern: angefangen von Cyberspionage zur Nachrichtengewinnung und Informationsmanipulation (APT37, Kimsuky, Sun Team) über verdeckte finanzielle Erpressung (APT38, Andariel) bis hin zu verschiedenen disruptiven und zerstörerischen Cyberoperationen (Lazarus-Gruppe).

Diese Angriffe nahmen erstmals im Zeitraum 2007–12 ernstzunehmende Ausmaße an. Damals entwickelte Nordkorea seine Schadprogramme der ersten Generation, die es in den Nordkorea zugeschriebenen Cyberangriffen „Operation Flame" und „1Mission" (2007–2012), „Operation Troy" (2009–2012), „Ten Days of Rain" (2011) und „Dark Seoul" (2013) einsetzte.[39] Diese richteten sich hauptsächlich gegen militärische und staatliche Ziele in Südkorea; Webseiten wurden gehackt, Informationen gestohlen und Distributed-Denial-of-Service-Angriffe durchgeführt.[40] So wurde beispielsweise eine Operation mit dem Namen „Ten Days of Rain" im März 2011 in Südkorea der nordkoreanischen Lazarus-Gruppe zugeschrieben.

33 David E. Sanger/William J. Broad: Trump Inherits a Secret Cyberwar Against North Korean Missiles, *New York Times*, 4. März 2017.

34 Martyn Williams: Catch Me If You Can: North Korea Works to Improve Communications Security, *38North-Website*, 12. April 2017; https://www.38north.org/2017/04/mwilliams041217.

35 MITRE ATT&CK Database: Lazarus Group, https://attack.mitre.org/groups/G0032/.

36 The National Cybersecurity and Communications Integration Center (NCCIC): HIDDEN COBRA – North Korean Malicious Cyber Activity, https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity.

37 Rosenberg/Beek 2019.

38 Group-IB 2017.

39 Novetta 2016.

40 Sherstobitoff/Laba/Walter 2018.

Tab. 1: Die nordkoreanischen Cyberaktivitätscluster auf der Basis von TTPs

APT Gruppe	Zielsektoren	Assoziierte Schadprogramme	Angriffsvektoren
APT 37 alias: Reaper, Group 123 Ricochet Chollima Scarcruft	Von 2014 bis 2017 richteten sich die Aktivitäten von APT37 vor allem gegen Behörden, das Militär, die Rüstungsindustrie und den Medien-sektor Südkoreas Seit 2017 richten sich die Angriffe auch gegen verschiedene Wirtschaftszweige in Japan, Vietnam und im Nahen Osten, u. a. Chemie, Elektronik, Verarbeitendes Gewerbe, Luft- und Raumfahrt, Automobilindustrie und Gesundheitswesen	APT37 nutzt eine breite Palette von Schadprogrammen für das anfängliche Eindringen und die anschließende Daten-Exfiltration. Ihre Schadprogramme zielen vor allem darauf ab, Informationen von Opfern zu stehlen, und viele sind so darauf ausgelegt, Daten von Interesse automatisch zu exfiltrieren. Neben maßgeschneiderten Schadprogrammen für Spionage-zwecke hat APT 37 auch Zugang zu zerstörerischer Malware.	Social-Engineering-Taktiken, die auf gewünschte Ziele zugeschnitten werden, strategische Web-Kompromittierungen, die typisch für gezielte Cyberspionage-Operationen sind, und die Nutzung von Torrent-Filesharing-Sites für die schnellere Verbreitung von Schadprogrammen
Kimsuky alias Velvet Chollima	Seit 2013 führt die Kimsuky-Gruppe in Südkorea eine Cyberspionage-Kampagne gegen staatliche Organisationen und Behörden durch, die mit Verteidigungsangelegenheiten zu tun hat, sowie gegen Institutionen und Unternehmen, die Südkorea in dem Konflikt mit Nordkorea unterstützen.	Schadprogramme, die in der Lage sind, den PC aus der Ferne zu kontrollieren, Tastenanschläge protokollieren, Dokumente entwenden und Dateiverzeichniseinträge sammeln. Der Name leitet sich von dem E-Mail-Konto »Kimsukyang« ab, das im Jahr 2013 als Ablage für gestohlene Daten genutzt wurde.	Spear-Phishing-Methoden – gezielte Cyberbetrugsmaschen, bei denen Nutzer auf Webseiten gelockt werden, die mit Schadprogrammen infiziert sind, oder bei denen PCs über angehängte Dateien infiziert werden, um auf diese Weise Zugriff auf das System und auf sensible Daten zu erhalten. Mit Schadprogrammen infizierte E-Mails, die als Einladung zu einer Pressekonferenz getarnt sind. Die jüngsten Aktivitäten der Kimsuky-Gruppe wurden im Februar 2019 festgestellt, im Vorfeld des zweiten Gipfeltreffens zwischen den USA und Nordkorea in Hanoi.
Sun Team	Nordkoreanische Überläufer und Journalisten in Südkorea	Android-Schadprogramme, die eine Hintertür-Datei in dem ausführ- und verknüpfbaren Format enthalten. Das Schadprogramm gibt sich als eine legitime App aus. Nach erfolgreicher Installation kopiert das Schadprogramm sensible Informationen einschließlich persönlicher Fotos, Kontakte und SMS-Nachrichten und schickt sie an diejenigen, die die Bedrohung geschaffen haben.	Eine sehr gezielte Kampagne, die 2017 begann und Facebook und KakaoTalk nutzte, eine der populärsten Chat-Apps in Südkorea, um mit Malware durchsetzte Phishing-Links an Zielpersonen zu schicken. Journalisten wurden mit gefälschten Nachrichten auf infizierte Webseiten gelockt.
Andariel – Lazarus-Untergruppe alias: Silent Chollima	Zunächst Cyberspionage gegen südkoreanische Militärbehörden, Rüstungsunternehmen, politische Organisationen, Sicherheitsunternehmen, IKT-Unternehmen und Energieforschungsinsti-tute; Ziele im Finanzsektor wie Geldautomaten, Banken, Reisebüros, Kryptowährungsbörsen und Nutzer von Online-Glückspielangeboten.	Nutzung bekannter Hintertüren, wie Aryan und Gh0st RAT, aber auch selbstentwickelter Backdoors wie Andarat, Andaratm, Rifdoor und Phandoor.	Spear-Phishing mithilfe von Makros, Wasserloch-Angriffe unter Ausnutzung von Active-X-Schwachstellen, Schwachstellen-Exploits in Sicherheits- und IT-gestützten Vermögensverwaltungssystemen und Angriffe auf Lieferketten.

Tab. 1 (fortgesetzt)

APT Gruppe	Zielsektoren	Assoziierte Schadprogramme	Angriffsvektoren
APT38 Bluenoroff Untergruppe von Lazarus alias: Stardust Chollima	Global – angegriffen werden ausschließlich Finanzinstitute, Casinos, Unternehmen, die Finanzsoftware entwickeln, und Kryptowährungsunternehmen. APT38 hat über 16 Organisationen in mindestens 11 Ländern angegriffen	Diese große und produktive Gruppe nutzt eine breite Palette maßgeschneiderter Schadprogrammtypen, u. a. Hinter-türen, Tunneler, Data Miner und zerstörerische Malware, um von Finanzinstituten Millionen von Dollar zu stehlen und die Netzwerke von Opfern funktionsuntüchtig zu machen.	Diese Gruppe geht sorgfältig und methodisch vor, und sie hat gezeigt, dass sie so lange, wie es notwendig ist, um das Netzwerk-Layout, die erforderlichen Genehmigungen und Systemtechnologien zu verstehen, Zugang zu den Environments von Angriffsopfern aufrechterhalten kann.
Lazarus-Gruppe alias: Labyrinth Chollima, Whois-Hacking Team	Global – Informationsdiebstahl und -spionage, Störung, Sabotage und finanzieller Gewinn; Aktivitäten der Lazarus-Gruppe konzentrieren sich darauf, die politischen Ziele des nordkoreanischen Regimes zu erreichen.	Die Gruppe hat im Lauf der Jahre zahlreiche Typen von Schadprogrammen eingesetzt, abhängig von den Angriffszielen und -zwecken. Lazarus nutzt verschiedene Techniken der Code-Obfuskation, schreibt ihre eigenen Algorithmen um, wendet kommerzielle Schutzsoftware an und nutzt eigene und Underground-Packprogramme. Die meisten Werkzeuge sind für einmalige Nutzung ausgelegt und werden nach ihrem Gebrauch durch eine neue Generation ersetzt.	Die Lazarus-Gruppe ist bereits seit 2009 aktiv. Ihre Schadprogramme wurden bei zahlreichen schwerwiegenden Cyberattacken entdeckt, etwa bei dem massiven Datenabgriffs- und Dateilöschungsangriff auf Sony Pictures Entertainment im Jahr 2014; bei der »Operation Troy« genannten Cyberspionage-Kampagne in Südkorea im Jahr 2013 und bei der Operation DarkSeoul, bei der 2013 südkoreanische Medien- und Finanzdienstleistungsunternehmen angegriffen wurden.

Quellen: Vom Autor zusammengestellte Tabelle, basierend auf den Cyberbedrohungsberichten FireEye Inc. 2018a und 2018b; Tarakanov 2013; Min 2018, Kaspersky Labs 2017, Ahnlab 2018 and 2019, Crowdstrike 2018, TrendMicro 2018; Novetta 2016.

Es handelte sich um einen groß angelegten DDoS-Angriff auf 40 südkoreanische Medienunternehmen, kritische Infrastruktur und finanzielle Websites sowie auf militärische Einrichtungen der USA.[41] Nach der Verabschiedung einer Resolution durch den UN-Sicherheitsrat (UNSCR 2087) und dem Überflug strategischer Bomber über Südkorea im März 2013 wurden bei „Dark Seoul" genannten Cyberangriffen, die Nordkorea zugeschrieben wurden, Computernetzwerke dreier Großbanken und der beiden größten Rundfunkanstalten Südkoreas – Korea Broadcasting System und Munhwa Broadcasting Corporation – zerstört. Sie wurden mit Viren infiziert, die Informationen stahlen und löschten.[42] In diesem Jahr verstärkte Nordkorea seine Cyberoperationen gegen Südkorea. Man führte eine Cyberspionage-Kampagne („Kimsuky") gegen südkoreanische Denkfabriken und Unternehmen durch, außerdem mehrere DDoS-Angriffe auf südkoreanische Medienunternehmen, staatliche Websites und Finanzdienstleistungsunternehmen.[43] Im Jahr 2016 ist Nordkorea wohl erfolgreich in die militärischen Netzwerke Südkoreas eingedrungen – dabei wurde das *Defense Integrated Data Center* des südkoreanischen *Cyber Commands* gehackt und 235 Gigabyte an geheimen militärischen Unterlagen einschließlich gemeinsamer Einsatzpläne für Kriegszeiten von US- und südkoreanischem Militär entwendet.[44]

In den Jahren 2014–15 hat Nordkorea angeblich seine Cyberdivisionen reorganisiert – Einheit 180 nahm jetzt Kryptowährungsbörsen ins Visier, Einheit 91 konzentrierte sich auf Cyberspionage von Technologien, die für die Entwicklung des nordkoreanischen Atom- und ballistischen Raketenprogramms benötigt werden, und Büro 121 konzentrierte sich auf Cyberoperationen gegen kritische

41 McAfee Labs 2011.

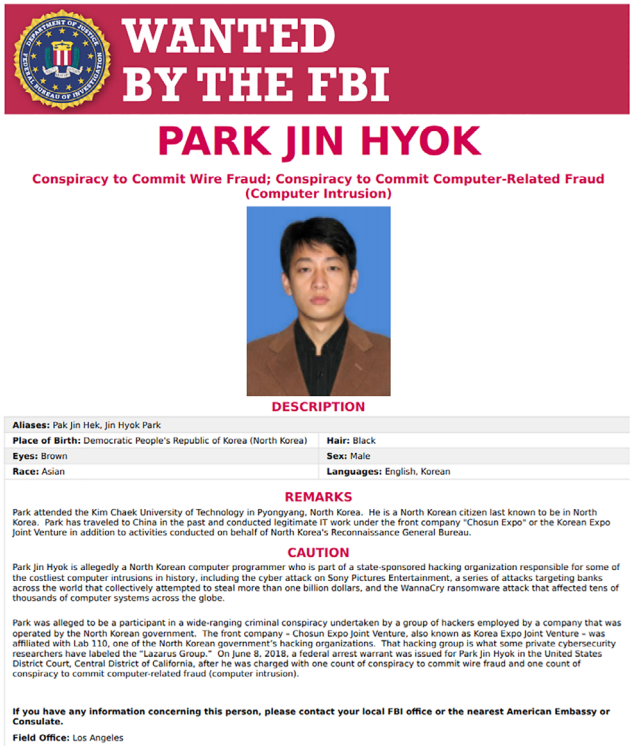
42 Choe Sang-Hun: Computer Networks in South Korea Are Paralyzed in Cyberattacks, *New York Times*, 20. März 2013; Michael Pearson/K.J. Kwon/Jethro Mullen: Hacking Attack on South Korea traced to China, Officials Say, *CNN*, 21. März 2013.

43 Tarakanov 2013.

44 Kyongae Choi: N. Korea likely Hacked S. Korea Cyber Command: Military, *Yonhap News*, 6. Dezember 2016; Christine Kim: North Korea Hackers Stole South Korea-U.S. Military Plans to Wipe out North Korea Leadership: Lawmaker, *Reuters*, 10. Oktober 2017.

Infrastruktur im Ausland – das Spektrum der Cyberziele und -operationen wurde nunmehr über Südkorea hinaus erweitert. So zogen nordkoreanische Hacker im Jahr 2014 internationale Aufmerksamkeit auf sich, als sie einen großangelegten Cyberangriff auf Sony Pictures Entertainment durchführten, bei dem 70 Prozent der Laptops und Computer von Sony Picture zerstört wurden. Ziel war es, das Unternehmen dazu zu zwingen, den Kinofilm „The Interview" nicht zu veröffentlichen.[45]

Im selben Jahr wurden nordkoreanischen Hackergruppen Angriffe auf Banken, die an das SWIFT-Finanznachrichtensystem angeschlossen sind, zugeschrieben; diese versuchten 951 Millionen Dollar von der Zentralbank von Bangladesch auf Konten in Sri Lanka und den Philippinen zu transferieren. Letztlich gelang es ihnen, 81 Millionen Dollar zu stehlen.[46] Seither ist Nordkorea mit einer Reihe von Cyberangriffen in Verbindung gebracht worden, die darauf abzielten, sich auf illegale Weise finanziell zu bereichern – so wurden im Februar 2017 zum Beispiel mehrere polnische Banken sowie die südkoreanische Kryptowährungsbörse Bithumb kompromittiert, wobei nordkoreanische Hacker 7 Millionen US-Dollar erbeuten konnten.[47] Im Dezember 2017 erklärten die Vereinigten Staaten, Großbritannien und Australien offiziell, Nordkorea stecke hinter dem globalen Angriff mit dem Erpressungstrojaner WannaCry, der über 200.000 Rechner in 150 Ländern infizierte, darunter auch Computer und Apparate in Krankenhäusern des *National Health Service* in England und Schottland.[48] Laut dem Bericht des Sachverständigengremiums des Nordkorea-Sanktionsausschusses der Vereinten Nationen, der im März 2019 veröffentlicht wurde, hat Nordkorea „zwischen Januar 2017 und September 2018 mindestens fünf erfolgreiche [Cyber-] Angriffe auf Kryptowährungsbörsen in Asien durchgeführt, die zu einem Gesamtverlust von 571 Millionen Dollar führten." In dem Bericht heißt es weiter: „Cyberangriffe durch [Nordkorea] in der Absicht, auf illegale Weise den Transfer von Geldern zu erzwingen, sind zu einem wichtigen Instrument der Umgehung von Sanktionen geworden, und sie sind seit 2016 immer komplexer und umfangreicher geworden".[49]



WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Pak Jin Hek, Jin Hyok Park	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean

REMARKS

Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. He is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted legitimate IT work under the front company "Chosun Expo" or the Korean Expo Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau.

CAUTION

Park Jin Hyok is allegedly a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the costliest computer intrusions in history, including the cyber attack on Sony Pictures Entertainment, a series of attacks targeting banks across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected tens of thousands of computer systems across the globe.

Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers employed by a company that was operated by the North Korean government. The front company - Chosun Expo Joint Venture, also known as Korea Expo Joint Venture - was affiliated with Lab 110, one of the North Korean government's hacking organizations. That hacking group is what some private cybersecurity researchers have labeled the "Lazarus Group." On June 8, 2018, a federal arrest warrant was issued for Park Jin Hyok in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer-related fraud (computer intrusion).

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles

Das FBI hat einzelne Nordkoreaner zur Fahndung ausgeschrieben

Gleichzeitig hat Nordkorea Cyberoperationen durchgeführt, um sich Zugriff auf kritische Infrastruktur in den Vereinigten Staaten und anderen Ländern weltweit zu verschaffen und diese auszuspähen – so hat Nordkorea zum Beispiel während des Nordkorea-USA-Gipfeltreffens im Jahr 2018 in Singapur eine Cyberexplorationskampagne durchgeführt, um in militärischen, finanziellen, Energie-, Telekommunikations-, Gesundheits- und anderen Netzwerken nach potenziellen Schwachstellen zu suchen.[50] Während Nordkorea sämtliche Vorwürfe, in illegale Hacker-Aktivitäten verwickelt zu sein, zurückgewiesen hat, scheint es sich zugleich weniger Mühe zu geben, seine Urheberschaft zu verschleiern: So hat man im Gefolge des Angriffs auf Sony relativ leicht durchschaubare „falsche Flaggen" verwendet, wie „Guardians of Peace", während bei früheren Angriffen auf südkoreanische Ziele andere Namen wie „New romantic Cyber Army Team" und „WhoIs Team" verwendet worden waren.[51] Laut dem südkoreanischen Defense White Paper 2014 „unterhält Nordkorea gegenwärtig eine 6.000 Mann starke Cyberkriegstruppe und führt Cyberangriffe durch, zum Beispiel um militäri-

45 Andrea Peterson: The Sony Pictures Hack, Explained, *The Washington Post*, 18. Dezember 2014; Greg Otto: U.S. charges North Korean hacker over Sony, WannaCry incidents, *Cyberscoop*, 6. September 2014.

46 Fraser/O'Leary/Cannon/Plan 2018; US Department of Homeland Security 2018.

47 Eduard Kovacs: Malware Attacks On Polish Banks Linked to Lazarus Group, *Security Week*, 13. Februar 2017.

48 Thomas Bossert: It's Official: North Korea Is Behind WannaCry, *The Wall Street Journal*, 18. Dezember 2017.

49 United Nations 2019, 51.

50 Sherstobitoff/Malhotra 2018.

51 Andy Greenberg: Russian Hacker False Flags Work – Even After They are Exposed, Wired Security, 27. Februar 2018; https://www.wired.com/story/russia-false-flag-hacks/.

Tab. 2: Chronologie der nordkoreanischen Cyberoperationen

03/2007	Laut Cybersicherheitsexperten, die an der **Operation Blockbuster** mitarbeiteten, beginnt die Lazarus-Gruppe damit, ihre **erste Generation von Schadprogrammen** zu entwickeln.
2009	**Die Lazarus-Gruppe** beginnt ihre **Operation Troy** und setzt erstmals ihre Wiper-Malware ein.
07/2009	Die Lazarus-Gruppe führte **Distributed-Denial-of-Service(DDoS)-Angriffe** gegen 17 südkoreanische und US-amerikanische Webseiten von Behörden durch.
03/2011	Die Lazarus-Gruppe führt im Rahmen einer Operation mit dem Namen **Ten Days of Rain** einen DDoS-Angriff gegen 40 südkoreanische Medienunternehmen, kritische Infrastrukturen und Finanz-Webseiten sowie auf US-Militäreinrichtungen in Südkorea durch.
03/2013	**Die Lazarus-Gruppe** setzt 32.000 Computer in südkoreanischen Rundfunkanstalten und Finanzdienstleistungsunternehmen außer Betrieb.
06/2013	Nordkorea wird ein **DDoS-Angriff gegen 69 südkoreanische Medienunternehmen** und behördliche Webseiten zugeschrieben.
09/2013	Kaspersky Lab entdeckt **eine Cyberspionage-Kampagne, die sogenannte Kimsuky-Kampagne,** gegen südkoreanische Denkfabriken und Unternehmen diverser Branchen.
2014	**Nordkorea wird ein Cyberangriff auf 140.000 Computer von Behörden und Unternehmen in Südkorea zugeschrieben,** gleichzeitig wird versucht, in das Steuerungssystem des südkoreanischen Verkehrsnetzes einzudringen. **APT37,** ein mit der nordkoreanischen Regierung assoziierter Cyberakteur, greift südkoreanische Medien und Webseiten über Flüchtlinge aus Nordkorea mit Wasserloch-Attacken an.
08/2014	**Nordkoreanische Hacker greifen den britischen Fernsehsender Channel 4 an.** Der Sender plante die Ausstrahlung einer Fernsehsendung über einen Atomwissenschaftler, der von Nordkorea entführt worden war. Die Sendung wurde nach dem Cyberangriff abgesetzt.
11/2014	**Die Lazarus-Gruppe greift Sony Entertainment Pictures** mit Wiper-Malware an. Die Gruppe nennt sich selbst »Guardians of Peace« und verlangt, dass eine Filmkomödie über eine Verschwörung zur Ermordung von Kim Jong-un nicht veröffentlicht wird. Die Gruppe stiehlt auch Informationen von Sony und veröffentlicht diese im Internet.
10/2015	Die Lazarus-Gruppe wird mit **Cyberangriffen gegen Banken auf den Philippinen** in Verbindung gebracht.
12/2015	Die Lazarus-Gruppe wird mit C**yberangriffen gegen die Tien Phong Bank in Vietnam** in Verbindung gebracht.
02/2016	Die Lazarus-Gruppe führt über das SWIFT-Nachrichtensystem einen **Cyberangriff auf die Zentralbank von Bangladesch** durch und stiehlt 81 Millionen US-Dollar.
04/2016	**Nordkoreanische Hacker dringen in das South Korean Defense Integrated Data Center ein** und stehlen geheime Unterlagen.
11/2016	**APT37** greift im Zuge einer Cyberspionage-Kampagne staatliche Institutionen und Finanzinstitute in Südkorea an.
2017	**Die Lazarus-Gruppe** infiltriert die Webseite der polnischen Finanzaufsichtsbehörde und infiziert Besucher mit Schadprogrammen.
02/2017	Nordkoreanische Hacker stehlen Kryptowährungen im Wert von 7 Millionen Dollar von der **Kryptowährungsbörse Bithumb**.
04/2017	Eine Reihe von **Spear-Phishing-E-Mails, die an US-amerikanische Rüstungsunternehmen geschickt werden,** werden der Lazarus-Gruppe zugeschrieben.
05/2017	**Der Kryptotrojaner WannaCry infiziert schätzungsweise 200.000 Rechner in über 150 Ländern.** Die Cybersicherheitsunternehmen Kaspersky Lab und Symantec behaupten, die Lazarus-Gruppe stehe hinter WannaCry. Die NSA schreibt den Kryptotrojaner WannaCry Nordkorea zu.
09/2017	**Die Lazarus-Gruppe greift Nutzer der Kryptowährungsbörse Coinlink** mit Spear-Phishing-E-Mails an.
2018	**Operation Sharpshooter** – Cyberoperationen mit dem Ziel, sich Zugriff zu kritischer Infrastruktur in den Vereinigten Staaten und anderen Ländern weltweit zu verschaffen, ein Cyberexploitationangriff, der militärische, finanzielle, Energie-, Telekommunikations-, Gesundheits- und andere Netzwerke auf potenzielle Schwachstellen absucht.

Quelle: Nach Baezner 2018

sche Operationen zu stören und auch gegen wichtige nationale Infrastruktureinrichtungen, um den Süden psychologisch und physisch zu lähmen".[52]

4 Bewertung der nordkoreanischen Cyberstrategien

Die obige Chronologie und die empirischen Daten deuten darauf hin, dass die nordkoreanischen Cybereinheiten während der letzten zehn Jahre drei verschiedene Entwicklungsphasen durchmachten, parallel zu den sich wandelnden politischen und ökonomischen Prioritäten des Regimes und den verfügbaren Ressourcen. Von 2009 bis 2011 richteten sich die nordkoreanischen Cyberoperationen hauptsächlich gegen Behörden und Finanzdienstleistungsunternehmen in Südkorea sowie gegen militärische Ziele und Rüstungsunternehmen in den USA; sie waren gekennzeichnet durch hacktivistische politische Botschaften und Bedrohungen. Der Angriff auf Sony, der hohe Wellen schlug, krönte diese Aktivitäten; es geschah zum ersten Mal, dass ein Nationalstaat ein Unternehmen angriff, um politische Ziele zu erreichen. Zwischen 2012 und 2015 konzentrierte sich Nordkorea auf Cyberspionage-Aktivitäten – etwa durch die Gruppen APT37 und APT38; dabei wurden südkoreanische und US-amerikanische Behörden, Rüstungsunternehmen, Universitäten und Denkfabriken sowie nordkoreanische Überläufer ins Visier genommen. Zwischen 2016 und 2018 begannen nordkoreanische Hackergruppen den Umfang und die Komplexität ihrer Operationen zu erweitern, sehr wahrscheinlich unter dem wachsenden Druck der finanziellen Sanktionen, und sie führten in zunehmendem Maße finanziell motivierte Cyberoperationen durch.[53]

Nordkorea hat in diesem Zusammenhang nach und nach seine Entschlossenheit zur Cybereskalation gezeigt – und dabei kritische Infrastrukturen anderer Nationalstaaten sowie Privatunternehmen und Banken ins Visier genommen; die politischen Motive dafür sind vielfältig – Vergeltung, Nötigung, verdeckte Nachrichtengewinnung und in zunehmendem Maße auch illegale finanzielle Gewinne, um strengere internationale Sanktionen zu umgehen und Devisen zu beschaffen. Von internationalen Normen hat es sich dabei nicht abschrecken gelassen.

Die grundlegende „Dialektik des nordkoreanischen Cyberraums" zeichnet sich durch eine Asymmetrie in Bezug auf Funktionalität und Verwundbarkeit aus – die nordkoreanische Internetinfrastruktur ist von den globalen Netzwerken abgekoppelt, und der gesamte Internetverkehr des Landes läuft über nur zwei Anbieter – die chinesische Unicom (40 %) und die russische TransTeleCom (60 %).[54] Ungeachtet der größer werdenden Intranet-Infrastruktur ist das Land nach wie vor weitgehend vom globalen Internet abgeschnitten, und die „Große Firewall" Chinas bietet eine „zusätzliche Barriere des Schutzes, der Zensur und der Überwachung für den nordkoreanischen Cyberspace".[55] Dies hat die Abhängigkeiten Nordkoreas und die potenziellen systemischen Schwachstellen für Vergeltungsmaßnahmen verringert und, was noch wichtiger ist, die Zuschreibungsrisiken reduziert.

Solange kein konventioneller Krieg ausbricht und keine konventionelle Eskalation stattfindet, werden zukünftige Konflikte auf der koreanischen Halbinsel wahrscheinlich in zunehmendem Maße aus parallelen und fortlaufenden Konfrontationen innerhalb des Cyberspace und aus diesem heraus sowie aus diversen Cyberangriffen sowohl durch staatliche als auch durch nicht staatliche Akteure bestehen. Cyber-basierte Informationskonflikte könnten schlimmstenfalls den Charakter „existenzieller Cyberangriffe" annehmen, die so umfassende Schäden anrichten, dass einer Regierung möglicherweise die Kontrolle über das Land entgleitet. Dabei würden auch erhebliche Teile der militärischen und kritischen Infrastruktur zerstört oder beschädigt: Stromerzeugung, Kommunikationsnetze, Brennstoffe und Verkehrswege, Notfalldienste, Finanzdienstleistungen usw.

Vermutlich werden solche Angriffe durch Desinformations-, Verschleierungs- und Täuschungskampagnen vorbereitet oder von diesen begleitet. Diese zielen darauf ab, die Wahrnehmungen und Überzeugungen der Bevölkerung des Ziellandes in einer bestimmten Weise zu beeinflussen, während sie die oberste politische Führung dieses Landes immer stärker unter Druck setzen, sodass diese Entscheidungen trifft, die, objektiv betrachtet, zu ihrer Niederlage führen – indem sie zum Beispiel zur Auflösung des Bündnisses zwischen den USA und Südkorea führen.

Sowohl die nord- als auch die südkoreanischen Online-Aktivitäten und Verhaltensweisen werden daher in zunehmendem Maße Offline-Folgen haben und umgekehrt. Die Trennlinien zwischen dem zivilen und dem militärischen Bereich, zwischen staatlichen und nicht staatlichen Akteuren, zwischen hauptsächlichen Zielen und eingesetzten Waffen werden zunehmend verschwimmen.

52 Republic of Korea, Ministry of National Defense 2014, 27.
53 FireEye Inc. 2019.
54 Peter Georgiev: North Korea Opens Second Internet Connection via Russia, *Transitions Online*, 16. April 2018.
55 Mansourov 2014.

In Krisenzeiten wird die besondere Eigenart asymmetrischer Cyberangriffe möglicherweise auch die Bereitschaft zu offensiven und unbeschränkten Cyberoperationen erhöhen, sofern die Einschätzung vorherrscht, dass die Entdeckungsrisiken gering sind, es keine Rechenschaftspflichten gibt und entsprechend die Wahrscheinlichkeit erfolgreicher Abschreckungsmaßnahmen der anderen Seite niedrig ist.

5 Politische Handlungsempfehlungen

Vor allem Südkorea muss eine Reihe von Schritten unternehmen, um Cyberoperationen umfassender als bisher in seine Militärstrategie und -doktrin zu integrieren. Im Jahr 2011 veröffentlichte das südkoreanische Verteidigungsministerium seine Cyberabwehrstrategie – das Rahmenkonzept für die Abwehr von Cyberbedrohungen (*Master Plan for Defense Cyber Policy*) mit vier zentralen Handlungsempfehlungen: Die südkoreanischen Gesetze sollten so modifiziert werden, dass sie Cyberoperationen erlauben; Cyber- und physische Operationen sollten in einer einheitlichen Militärdoktrin – dem „Handbuch für Teilstreitkräfte-übergreifende Cyberoperationen" – zusammengeführt werden; im Zuständigkeitsbereich des Vereinigten Oberkommandos der südkoreanischen Streitkräfte sollte ein Cyberkommando eingerichtet werden, und schließlich sollten Frühwarn- und Krisenbewältigungsmechanismen für Cyberkrisen geschaffen werden.[56]

Mittlerweile hat Südkorea die zivil-militärische Zusammenarbeit im Cyberbereich verbessert; dazu gehören auch gemeinsame Programme mit dem Ministerium für Wissenschaft, Informationstechnologien und Zukunftsplanung und dem Nationalen Nachrichtendienst (NIS), in der Absicht, eine potenzielle Cyberreservetruppe zu schaffe; zudem gehören eine engere Koordinierung der nachrichtendienstlichen Grenzüberwachung, gemeinsame Reaktionen auf die elektronische Kriegführung Nordkoreas und die Störung von GPS-Signalen sowie ein spezieller Plan zur Verbesserung von Kampffähigkeiten unter Kriegsbedingungen dazu.

Abgesehen von diesen Maßnahmen im Inland sollte Seoul auch gemeinsamen Anstrengungen mit dem US-Militär Priorität einräumen, um sicherzustellen, dass das Bündnis Cyberoperationen so effektiv wie möglich durchführt. In jüngerer Zeit sind die südkoreanischen Cyberfähigkeiten in das strategische Rahmenkonzept des Bündnisses zwischen den USA und Südkorea aufgenommen worden; hierbei geht es darum, durch gemeinsame Programme zur Entwicklung KI-basierter Technologien ein breites Spektrum von Cyberbedrohungen abzuwehren.[57]

Die zentrale Herausforderung für die Zukunft der Allianz zwischen den USA und Südkorea wird jedoch darin bestehen, sich auf potenzielle Veränderungen des Charakters der Kriegführung einzustellen. Seit Anfang der 1990er-Jahre hat Südkorea sein Militär umfassend modernisiert, um auf das größer werdende Spektrum nordkoreanischer Bedrohungen zu reagieren, technologische und Interoperabilitätsdefizite gegenüber den US-Streitkräften zu verringern und auf lange Sicht die Fähigkeit zu erreichen, sich aus eigener Kraft zu verteidigen. Im Zuge dessen haben die südkoreanischen Verteidigungsplaner nach einem neuen strategischen Paradigma und operativen Konzepten gesucht, die unter Bedingungen strategischer Ungewissheit eine größere Flexibilität, Anpassungsfähigkeit und Autonomie erlauben.

Aufgrund des ambitionierten Umfangs, der zeitlichen Vorgaben und der relativ hohen Kosten haben verteidigungspolitische Reformvorhaben in Südkorea fortwährende politische Debatten über die Machbarkeit, Bezahlbarkeit, das Tempo, die Richtung, den Charakter und die Implementierung der Reformvorschläge ausgelöst. Diese politischen Debatten drehten sich um fünf zentrale Herausforderungen für die Verteidigungsplanung Südkoreas: (1) Wie lassen sich die gegenwärtigen operativen Anforderungen gegenüber Nordkorea einerseits und die notwendige Vorkehrungen für relativ ungewisse zukünftige regionale Bedrohungen andererseits ausbalancieren und priorisieren? (2) Wie lässt sich sicherstellen, dass in der Gegenwart und in der Zukunft die für die Umsetzung ausgewählter verteidigungspolitischer Reformen notwendigen Haushaltsmittel in ausreichendem Umfang bereitgestellt werden? (3) Wie lassen sich die südkoreanischen Streitkräfte organisatorisch straffen und verkleinern, ohne ihre operative Bereitschaft und ihre Fähigkeiten zu verringern? (4) Wann ist der richtige Zeitpunkt, um die operative Führung (OPCON) in Kriegszeiten, die gegenwärtig bei den US-Streitkräften liegt, auf Südkorea zu übertragen, ohne dass die Abschreckung dadurch beeinträchtigt wird? (5) Wie sollte der zukünftige strategische Rahmen der Allianz zwischen den USA und Südkorea aussehen?[58]

Anders gesagt: Die relativ ambitionierten, aber auch sachgerechten verteidigungspolitischen Reformvorha-

56 Republic of Korea, Ministry of National Defense 2014.

57 Lee 2016, 70.

58 Raska 2016a, 32.

ben Südkoreas in den vergangenen beiden Jahrzehnten standen in scharfem Kontrast zu den vorherrschenden politischen, strategischen und operativen Realitäten, wie etwa gegensätzlichen Einschätzungen von Verteidigungserfordernissen, der strukturellen Abhängigkeit von der Allianz zwischen USA und Südkorea, einer statischen, defensiven Verteidigungsstrategie und Rivalitäten zwischen den Teilstreitkräften innerhalb der Organisationsstruktur der Streitkräfte, die die Relevanz traditioneller Sicherheitskonzepte und der herkömmlichen strategischen Kultur gestützt haben. Das südkoreanische Militär wurde nicht tiefgreifend restrukturiert. Vielmehr kam es zu einer allmählichen Umstellung von der operativen und militärtechnologischen Nachahmung amerikanischer Fähigkeiten hin zu einer selektiven Anpassung der Fähigkeiten in dem schrittweisen, evolutionären Prozess der Modernisierung der Streitkräfte.

Trotz gemeinsamer Anstrengungen zur Behebung bestehender Technologie- und operativer Defizite im Zusammenhang mit der Interoperabilität mit US-Streitkräften, insbesondere in den Bereichen Luftwaffe, C4ISR und Cyberoperationen, sowie mit der Interoperabilität zwischen den drei südkoreanischen Teilstreitkräften haben die südkoreanischen Verteidigungsreformen weder die „kognitive Matrize“ noch die Organisationsstruktur des südkoreanischen Militärs erheblich verändert. Die südkoreanischen Streitkräfte sind nicht vollständig in der Lage gewesen, ihr militärtechnologisches Potenzial mit den erforderlichen organisatorischen, konzeptionellen und operativen Neuerungen in ihre Modernisierungsstrategie in einer Weise zu integrieren, die es ihnen ermöglicht hätte, fortgeschrittene Technologien einschließlich Cyberfähigkeiten in neuer Weise zu nutzen.[59] Unter diesen Bedingungen hat sich Nordkorea nach und nach einen strategischen Vorteil verschafft, indem es in Zusammenhang mit seinem Atom- und seinem ballistischen Raketenprogramm Cyberfähigkeiten als asymmetrische Fähigkeiten entwickelte, die ein relativ kostengünstiges, effektives Mittel sind, um seinen Einfluss geltend zu machen und um politischen, wirtschaftlichen und militärischen Zwang auszuüben, ohne einen größeren bewaffneten Konflikt auszulösen.

59 Raska 2016b, 95–130.

Literatur

AhnLab (2018): *Full Discloser of Andariel: A Subgroup of Lazarus Threat Group.* Gyeonggi-do, South Korea: AhnLab Analysis Report, 23. Juni; https://jp.ahnlab.com/global/upload/download/techreport/[AhnLab]Andariel_a_Subgroup_of_Lazarus%20(3).pdf;

AhnLab (2019): Operation Kabar Cobra: Tenacious Cyber-Espionage Campaign by Kimsuky Group. Gyeonggi-do, South Korea: AhnLab Analysis Report, 28. Februar; https://jp.ahnlab.com/global/upload/download/techreport/[Analysis_Report]Operation%20Kabar%20Cobra%20(1).pdf

Baezner, Marie (2018): *Cyber Disruption and Cybercrime: Democratic People's Republic of Korea.* Zürich: Center for Security Studies (CSS), ETHZ

Bermudez, Joseph (2010): *A New Emphasis on Operations Against South Korea? A Guide to North Korea's Intelligence Reorganization and the General Reconnaissance Bureau.* Washington, D.C.: *38 North Special Report*; https://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf

Bermudez, Joseph (2016): *North Korea Reorganizes Security Services.* London: IHS Jane's; https://www.janes.com/images/assets/196/66196/North_Korea_reorganises_security_services.pdf

Boo, Hyeong-wook (2017): An Assessment of North Korean Cyber Threats, *The Journal of East Asian Affairs*, 31 (1), 97–117

Boo, Hyeong-wook et. al. (2013): *A Study on Future Direction of Defense Cyber Policy*. Korean Institute for Defense Analysis report (*in Koreanisch*) S. 94

Crowdstrike (2018): *Global Threat Report 2018.* Sunnyvale, Cal: A Crowdstrike Special Report; https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf

FireEye Inc. (2018a): *APT 38 – Un-usual Suspects.* Milpitas, Cal.: FireEye Report, 2018; https://content.fireeye.com/apt/rpt-apt38

FireEye Inc. (2018b): *APT37 (Reaper) The Overlooked North Korean Actor.* Milpitas, Cal.: A FireEye Special Report; https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

FireEye Inc. (2019): *M-Trends 2019.* Milpitas, Cal.: FireEye Mandiant Services Special Report, https://content.fireeye.com/m-trends

Fraser, Nalani/O'Leary, Jacqueline/Cannon, Vincent/Plan, Fred (2018): APT38: *Details on New North Korean Regime-Backed Threat Group.* Milpitas, Cal.: FireEye Threat Research Report, 3. Oktober; https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html

Group-IB (2017): *Lazarus Arisen: Architecture, Tools, Attribution.* Singapore/Moscow: Group-IB Investigation Report, 30. Mai; https://www.group-ib.com/blog/lazarus

Jun, Jenny/LaFoy, Scott/Sohn, Ethan (2015): North Korea's Cyber Operations: Strategy and Responses. Washington, D.C.: Center for Strategic and International Studies

Kasperksy Labs (2017): *Lazarus under the Hood.* Moscow: A Kaspersky Forensic Investigation Report; https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf

Kong, Ji Young, Lim, Jong In, and Kim, Kyoung Gon (2019): The All-Purpose Sword: North Korea's Cyber Operations and Strategies, 11th International Conference on Cyber Conflict,

https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf

Lee, Chung Min (2016): *Enhancing US Power Projection*, in: Patrick Cronin (ed.): Breakthrough on the Peninsula: Third Offset Strategies and the Future of Defense of Korea. Washington D.C.: Center for New American Security S. 70, https://www.cnas.org/publications/reports/breakthrough-on-the-peninsula

Lee, Duri (2017): *How to Improve the ROK and U.S. Military Alliance Against North Korea's Threats to Cyberspace: Lessons From NATO's Defense Cooperation*. Monterrey, Cal.: Naval Postgraduate School; Master of Science Thesis in Information Strategy and Political Warfare (Dezember)

Mansourov, Alexander (2014): *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance*. Seoul: Korean Economic Institute, KEI Academic Paper Series

McAfee Labs (2011): *Ten Days of Rain – Expert Analysis of Distributed Denial-of-Service Attacks Targeting South Korea.* Santa Clara, Cal.: McAffee White Paper, Juli; https://securingtomorrow.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf

Min, Jaewon (2018): *North Korean Defectors and Journalists Targeted Using Social Networks and KakaoTalk*, McAfee Labs Blog, 11. Januar; https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/north-korean-defectors-journalists-targeted-using-social-networks-kakaotalk/

Novetta (2016): *Operation Blockbuster: Unraveling the Long Thread of the Sony Attack.* McLean, Va.: Novetta Special Report; https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

Pinkston, Daniel A. (2016): Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the Son'gun Era, *Georgetown Journal of International Affairs*, 27 (3), 60–76

Raska, Michael (2016a): *South Korea's Military Innovation Trajectories*, in: Patrick Cronin (ed.): *Breakthrough on the Peninsula: Third Offset Strategies and the Future of Defense of Korea.* Washington D.C.: Center for New American Security

Raska, Michael (2016b): *Military Innovation in Small States: Creating a Reverse Asymmetry.* New York: Routledge

Republic of Korea, Ministry of National Defense (2012): *2012 Defense White Paper*. Seoul: MoD

Republic of Korea, Ministry of National Defense (2014): *2014 Defense White Paper*. Seoul: MoD

Rosenberg, Jay/Beek, Christiaan (2019): *Examining Code Reuse Reveals Undiscovered Links among North Korea's Malware Families.* Santa Clara, Cal.: McAfee Labs Report, 9. August; https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/examining-code-reuse-reveals-undiscovered-links-among-north-koreas-malware-families

Sherstobitoff, Ryan/Laba, Itai/Walter, James (2018): *Dissecting Operation Troy: Cyberespionage in South Korea.* Santa Clara, Cal.: McAfee White Paper, 4. Mai; https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf

Sherstobitoff, Ryan/Malhotra, Asheer (2018): *Operation Sharpshooter Targets Global Defense, Critical Infrastructure.* Santa Clara, Cal.: McAfee Labs, 12. Dezember; https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/

Tarakanov, Dmitri (2013): *The 'Kimsuky' Operation: A North Korean APT?* Moscow: Kaspersky APT Reports, 11. September 2013, https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/

Tosi, Scott (2017): North Korean Cyber Support to Combat Operations, *Military Review*, (4), 43–51

Trend Micro (2018): *A Look Into the Lazarus Group's Operations.* Irving, Texas: Trend Micro Cybercrime and Digital Threats Blog, 24. Januar; https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations

United Nations (2019): *Report of the Panel of Experts established pursuant to resolution 1874 (2009)*, New York: United Nations, S/2019/171, 5. März.

US Department of Homeland Security (2018): *HIDDEN COBRA – FASTCash Campaign*. Washington, D.C.: National Cybersecurity and Communications Integration Center, 2. Oktober; https://www.us-cert.gov/ncas/alerts/TA18-275A