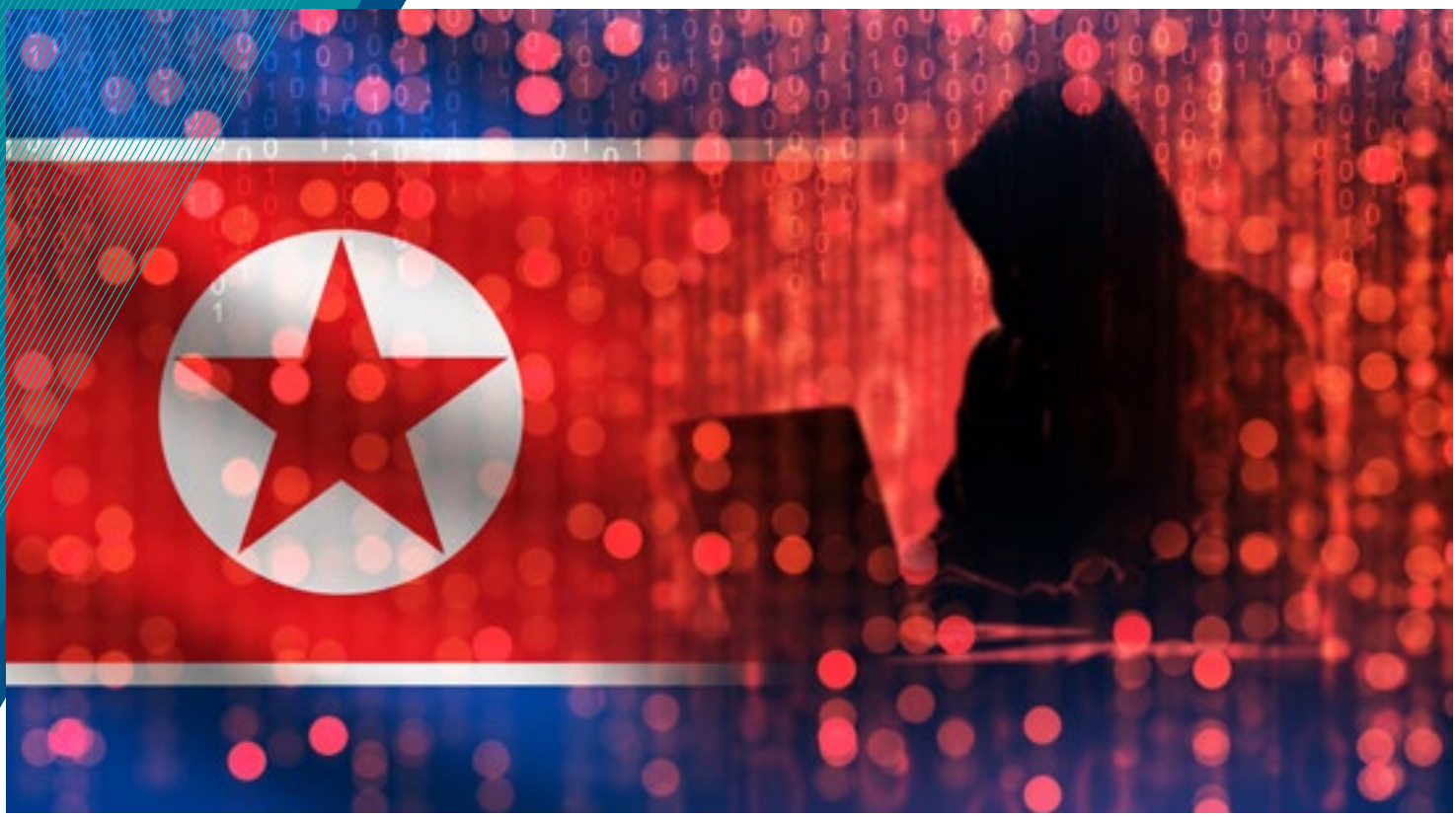
Nr. 523 / Februar 2024
Analysen & Argumente

KONRAD ADENAUER STIFTUNG



Cyber-Actors: Nordkorea

Wie Cyberoperationen das staatliche System stützen

Lukas Joselewitsch

- Nordkoreanische Einheiten konzentrieren sich vornehmlich auf politische und wirtschaftliche Spionage sowie die Beschaffung von Devisen. Disruptive Angriffe sind aktuell eher unwahrscheinlich.
- Die generierten Finanzmittel dienen primär der politisch-ökonomischen Stabilisierung des Staates sowie dem Ausbau nuklearer und konventioneller Militärfähigkeiten.
- Bisher wurden circa drei bis sechs Milliarden US-Dollar (ohne Dunkelziffer) durch den Einsatz von Cybermitteln gewonnen.
- Den Aktivitäten kann durch Detektion und Veröffentlichung von nordkoreanischen Vorgehensweisen sowie Aufklärung potenzieller Zielinstitutionen entgegengewirkt werden.
- Nordkoreanische Einheiten agieren opportunistisch und flexibel. Es ist zu erwarten, dass die Angriffe trotz Gegenmaßnahmen anhalten werden. Bisweilen besteht keine nennenswerte Gefahr für Deutschland.

Inhaltsverzeichnis

Die Demokratische Volksrepublik Korea (DVRK) hat in den letzten Jahren den Cyber- und Informationsraum zunehmend zur Umsetzung der staatspolitischen Agenda instrumentalisiert und schöpft hierbei das gesamte Spektrum möglicher Operationsziele aus: Sabotage und Disruption, *Signaling*, politische Spionage, Wirtschaftsspionage, Devisenbeschaffung und Propaganda. Laut Kim Jong-un fungieren Cyberangriffe neben Kernwaffen als „Allzweckschwert" zur Erfüllung der Ziele des Regimes.

Ziele und Wirkung

Einheiten der DVRK haben wiederholt disruptive Angriffe zur Sabotage und Störung von feindlichen Systemen unternommen, um politische Konzessionen von Südkorea und den USA zu erzwingen oder als Instrument politischer Signalwirkung: bisher erfolglos. Nennenswerte Beispiele in diesem Zusammenhang waren verschiedene Operationen gegen IT-Systeme in Südkorea wie die Operation *Dark Seoul*[1] und *Ten Days of Rain*, die zu weitreichenden Störungen im Land führten. Nach 2014 wurden keine vergleichbaren Aktivitäten beobachtet; es ist davon auszugehen, dass offensive Cyberaktivitäten als Mittel der Zwangsdiplomatie nur wenig Wirkkraft hatten. Somit ist anzunehmen, dass etwaige Operationen außerhalb eines militärischen Szenarios vorerst nicht durch die DVRK ausgeführt werden.

Politische Spionage war bisher primär gegen zivile und öffentliche Einrichtungen Südkoreas sowie gegen internationale Organisationen und ausländische Individuen gerichtet. Ziel der Operationen ist die Gewinnung strategisch und sicherheitspolitisch relevanter Informationen. In den letzten Jahren kam es z. B. zu einem Angriff gegen elf UN-Sicherheitsrats Mitglieder, um Informationen zu Sanktionsbeschlüssen zu gewinnen.[2] Ferner wurden internationale Think-Tanks sowie Journalistinnen und Journalisten kompromittiert, um Informationen zur ausländischen Lageeinschätzung der DVRK zu erhalten.[3] Die genannten Aktivitäten laufen weiter fort und passen sich flexibel an die politischen Interessen des Regimes an. Es ist nicht davon auszugehen, dass Nordkorea von der politischen Spionage absehen wird.

Hinsichtlich wirtschaftlich motivierter Spionageaktivitäten führt die DVRK Operationen aus, um Informationen zu ökonomisch relevanten Sektoren zu generieren. Hauptziel waren in der Vergangenheit internationale Rüstungsunternehmen, mit dem Ziel, technische Informationen zur Entwicklung moderner Waffensysteme – unter anderem Kernwaffen – zu gewinnen.[4] Während der Covid-19 Pandemie 2020 bis 2022 hat der Staat jedoch auch Impfstoffhersteller im Ausland angegriffen, um die autarke Impfstoffproduktion der DVRK zu ermöglichen. Die Wirtschaftsspionage gleicht in ihrem Kalkül der politischen Spionage und richtet sich nach den strategischen Zielen der Staatsführung. Es ist zu erwarten, dass die DVRK zukünftig unter anderem vermehrt Angriffe gegen Satellitentechnologieunternehmen ausführen wird, um jüngste Bestrebungen zur Produktion weltraumgestützter Waffen- und Aufklärungssysteme zu untermauern.

Spionage von internationalen Rüstungsunternehmen war ein Hauptziel.

Finanziell motivierte Angriffe zur Gewinnung von Devisen konnten seit circa 2011 beobachtet werden. Das Vorgehen der Akteure war anfangs vornehmlich auf niedrigschwellige Ziele wie Spieleplattformen ausgerichtet. Ab 2015 ließ sich jedoch ein Anstieg der Aktivitäten in Qualität und Quantität verzeichnen. Die DVRK erregte internationales Aufsehen mit komplexen Angriffskampagnen gegen Finanzinstitutionen: Kompromittierung des internationalen SWIFT-Zahlungssystems und Angriffe auf den Auszahlungsmechanismus von Bankautomaten sowie die globale Ransomwarekampagne *WannaCry*.[5] Die Angriffe gegen den Finanzsektor generierten circa zwei Milliarden US-Dollar, die Ransomwareaktivitäten führten zur Verschlüsselung von 230.000 Systemen in 150 Ländern.

Kryptowährungsplattformen sind im Fokus.

Als Reaktion auf die Operationen wurde die Vorgehensweise der DVRK durch international kooperierende Cybersicherheitsinstitutionen offengelegt und entsprechende Schutzmechanismen konnten bereitgestellt werden. Dies hatte zur Folge, dass die Lukrativität der Angriffe wesentlich geschmälert wurde und die DVRK ihre Strategie neu ausrichten musste. Seitdem konzentrieren sich die Angreiferinnen und Angreifer vermehrt auf nichtstaatliche Kryptowährungsplattformen, die sich bis heute als profitables und bevorzugtes Ziel erweisen. Die Plattformen weisen oftmals einen geringen Sicherheitsstandard auf und erregen im Falle einer Kompromittierung weniger öffentliches Aufsehen als eine Bank. Im Rahmen der Operationen verschaffen sich die Hackerinnen und Hacker der DVRK Zugriff auf digitale Bankkonten und transferieren die Kryptowährung auf ein nordkoreanisches *Wallet*. Im Abschluss wird die Währung durch verschiedene Mechanismen gewaschen und in Fiatwährung umgewandelt. Seit 2015 konnte die DVRK auf diesem Wege schätzungsweise drei bis sechs Milliarden US-Dollar generieren. Es lässt sich jedoch annehmen, dass die Dunkelziffer weitaus höher ist. 2020 sollen 1,7 Milliarden US-Dollar durch maliziöse Angriffe gewonnen worden sein. Neben dem Einsatz der *WannaCry*-Schadsoftware[6] sind keine finanziell motivierten Angriffe gegen deutsche Ziele bekannt.

Beweggründe

Die DVRK verfügt über keine offizielle Cyberdoktrin, die Einblick in das strategische Kalkül der staatlichen Führung gibt. Die Motive des Regimes lassen sich jedoch aus der politischen Situation des Staates, den Spezifika des Cyberraumes und den offiziellen Staatszielen ableiten.

Pjöngjang sieht sich immanent durch die militärische Präsenz und Allianz der USA mit Südkorea bedroht. Dies ist zentraler Treiber für die Ausführung disruptiver Angriffe. Entsprechende Cybermittel können im Falle einer militärischen Auseinandersetzung als Instrument asymmetrischer Kriegsführung genutzt werden. In Friedenszeiten dient der Cyberraum dem Regime zur Ausführung von Angriffen gegen andere Staaten, ohne dabei eine Eskalation mit konventionellen Waffensystemen zu riskieren. Diese Strategie der „tausend Nadelstiche" dient der Machtdemonstration, der Generierung von dringend benötigten Finanzmitteln sowie der innen- wie außenpolitischen Legitimierung der Staatsführung.

Der nordkoreanische Staat ist aufgrund ökonomischer Insuffizienz, internationaler Sanktionen und einem hohen Warenimportbedarf auf Devisen angewiesen, um die interne Ökonomie aufrecht zu erhalten, Luxusgüter für die Elite zu finanzieren sowie nukleare und konventionelle Rüstungskapazitäten weiter auszubauen.

Seit 1970 nutzt das Regime klandestine und illegale Methoden zur Fremdwährungsbeschaffung. Cyberangriffe stellen in diesem Zusammenhang mittlerweile das scheinbar lukrativste Instrument dar, um dem wirtschaftlichen Defizit entgegenzuwirken. Zum einen lässt sich dies auf den Rückgang konventioneller Methoden zurückführen. So wurden Falschgeld-

produktion, Schmuggel und moderne Sklaverei von nordkoreanischen Staatsbürgerinnen und -bürgern im Ausland intensiv durch die internationale Staatengemeinschaft bekämpft.[7] Darüber hinaus lässt sich eine Korrelation zwischen den gestiegenen Investitionen in das Kernwaffenprogramm und der steigenden Quantität und Qualität der Cyberoperationen erkennen. Die Beschaffungstaktiken im Cyberraum lassen sich aufgrund der Intransparenz und Immaterialität der Domäne nur schwer unterbinden. Akteure können unerkannt und weitestgehend straffrei agieren sowie Vorwürfe plausibel abstreiten. Darüber hinaus fällt das Kosten-Nutzen-Verhältnis zu Gunsten der Angreiferinnen und Angreifer aus. Aktive Gegenmaßnahmen (wie *Hackbacks*) gegen die DVRK sind überwiegend wirkungslos, da Nordkorea aufgrund einer geringen Digitalisierung kaum Angriffsfläche bietet. Es wird vermutet, dass die USA vereinzelt Angriffsinfrastrukturen Nordkoreas gestört haben, jedoch ohne erkennbaren Erfolg.

Cyberangriffe als lukratives Mittel um finanzielle Engpässe des Staates auszugleichen.

Um einen theoretischen Einblick in die Motivation des Staates zu erhalten, ist die *Songun-Doktrin* (Militär zuerst), die seit 2009 das politische Handeln des Regimes bestimmt, essenziell. Die Doktrin priorisiert die Verteidigungsbereitschaft der Nation angesichts der wahrgenommenen Bedrohung. Staatliche Mittel werden vornehmlich in den Verteidigungsapparat der DVRK investiert, in dessen Zentrum das Kernwaffenprogramm steht. Grundgedanke der *Songun-Doktrin* ist die Wechselwirkung zwischen einem starken Militär und wirtschaftlicher Prosperität. Der Doktrin zufolge soll eine potente Rüstungsindustrie genug finanzielle Mittel durch Exporte von Rüstungsgütern generieren und gleichzeitig die territoriale Integrität des Staates gewährleisten. Die Eliten des Landes, die auch die Cybereinheiten umfassen, sind offiziell vornehmlich im Verteidigungssektor tätig. Es ist folglich im Sinne der Doktrin, dass die Mehrheit der Investitionen und Wirtschaftsspionageoperationen der Förderung des Militärs dient.

Organisation

Die Organisation der nordkoreanischen Cybergruppierungen lässt sich aufgrund verschiedener widersprüchlicher Angaben nicht klar bestimmen. Es ist jedoch bekannt, dass die Cybereinheiten der Koreanischen Volksarmee unterstehen, dessen Oberbefehlshaber der „Oberste Führer" Kim Jong-un ist. Die Mehrheit der bekannten Akteure soll im *Bureau 121* des Militärgeheimdienstes Generalbüro für Aufklärung (RGB) angesiedelt sein. Zu den hier verordneten Einheiten zählen u. a. die *Lazarus Gruppe, Bluenorrof* und *Kimsuky*.[8] Es ist ebenfalls möglich, dass Teile des Cyberapparates dem Ministerium für Staatssicherheit unterstehen. Von zentraler Bedeutung neben dem RGB ist das *Bureau 39*, das für die konventionelle Generierung von finanziellen Mitteln zuständig sein soll. Aufgrund der gemeinsamen Zielsetzung der Organisationen ist davon auszugehen, dass eine operative Zusammenarbeit besteht. Jüngst konnte ein Wandel in der Organisation und Zuständigkeit der Akteure beobachtet werden. Während in der Vergangenheit die Gruppierungen autark voneinander operiert haben, lässt sich seit 2022 eine Vermischung der Einheiten erkennen. Es findet ein Austausch von Zuständigkeiten und Instrumenten unter den Akteuren statt, die auf ein verändertes (arbeitsteiliges), effizienteres und ressourcenschonenderes Zusammenwirken schließen lassen. Die Aus- und Fortbildung der Einheiten erfolgt sowohl an Universitäten der DVRK als auch in China.[9] Ein wesentliches Merkmal der nordkoreanischen Cyberorganisation ist die strategische Stationierung von Einheiten, die als IT-Fachkräfte im Ausland getarnt sind. Die Akteure operieren von ihrem jeweiligen Standort aus, was die Zuordnung erschwert und staatliche Kosten senkt.

Ausblick

Das nordkoreanische Regime wird auch weiterhin und künftig wohl noch stärker Operationen im Cyberraum verfolgen, um staatliche Ziele zu erreichen. Insbesondere finanziell motivierte Operationen und Spionage sind mittlerweile ein essenzielles Instrument der Staatspolitik. Die grundlegenden Motive sind dabei auch in dem doktrinären System der DVRK verankert. Das Raketen- und Atomprogramm des Landes erfordert hohe Investitionen und technische Informationen. Gleichzeitig gerät der Staat durch seine wirtschaftlichen Probleme zunehmend in Bedrängnis. Daher ist es schwer vorherzusagen, wie sich die volatile und impulsive Politik des Regimes in Zukunft entwickeln wird. Sofern sich Angriffe auf digitale Konten, Kryptomarktplätze oder digitale Finanzströme weiterhin als lukrativ erweisen, ist nicht davon auszugehen, dass Pjöngjang auf die Devisenbeschaffung durch gezielte Cyberoperationen verzichten wird. Eine Zusammenarbeit zwischen Einheiten der DVRK und politischen Verbündeten wie Russland, China oder dem Iran ist bisweilen nicht zu beobachten. Zwischenstaatliche Kooperationen im Cyberraum erfordern ein hohes Maß an Koordination und operativer Integration, die in Anbetracht der aktuellen politischen Interessen des Regimes eher unwahrscheinlich sind. Für die Bundesrepublik Deutschland stellt das Agieren der DVRK im Cyberraum bisher keine besondere Bedrohung dar. Jedoch könnte schon die kleinste Erosion der aktuell angespannten diplomatischen Verhältnisse zwischen der DVRK, Südkorea und den USA verheerende Folgen für die globale sicherheitspolitische Lage bedeuten. Die Vereinten Nationen haben bereits 2019 entsprechende Schritte wie intensivierte Sanktionen, öffentliches *Naming and Shaming* sowie verstärkte transnationale Zusammenarbeit eingeleitet, um die Wirkkraft der Angriffe und ihrer politischen Effekte einzudämmen.[10] Es ist wahrscheinlich, dass schwankende Kryptowährungspreise oder verstärkte Sicherheitsmaßnahmen der Plattformen den Angriffen entgegenwirken können. Die Sicherheitsbehörden konzentrieren sich bisher auf die Detektion und Veröffentlichung von nordkoreanischen TTPs (*Tactics, Techniques and Procedures)*. Dieses Vorgehen und eine weite Streuung von angreiferbezogenen Informationen hat sich bisweilen als effektivstes Mittel zur Mitigierung der Angriffe erwiesen. Aufgrund der hohen Bedeutung für Staatsdoktrin und Finanzen ist jedoch davon auszugehen, dass die DVRK ihre Methoden anpassen und nach neuen Wegen suchen wird. Aktuell gilt es folglich, das Vorgehen zu beobachten, die Resilienz der Angriffsziele zu stärken und die Beschaffungsmethoden im digitalen sowie kinetischen Raum bestmöglich mit internationalen Partnern zu unterbinden.

Zum jetzigen Zeitpunkt sind die Akteure der DVRK nur bedingt relevant für Deutschland. Bisher waren wenige nennenswerte Angriffe gegen regionale Ziele zu beobachten. Eine zukünftige operative Priorisierung Deutschlands lässt sich aktuell nicht erkennen.

1 Mehr hierzu unter: https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/operation-troy-dark-seoul/.

2 Vgl. https://media.defense.gov/2023/Jun/01/2003234055/-1/-1/0/JOINT_CSA_DPRK_SOCIAL_ENGINEERING.PDF.

3 Vgl. https://www.zdnet.com/article/north-korea-has-tried-to-hack-11-officials-of-the-un-security-council/.

4 Ein Beispiel hierfür ist der Angriff gegen einen russischen Produzenten von ballistischen Raketen.

5 In 2017 erfolgte eine massive Ransomwarekampagne unter dem Namen *WannaCry*, bei der Systeme verschlüsselt und lediglich gegen eine Lösegeldsumme von 300 US-Dollar wieder entschlüsselt wurden.

6 Die sich selbst replizierende Ransomware infizierte 2017 Teile der deutschen IT und richtete merklichen Schaden an. Es ist davon auszugehen, dass die DVRK die Kontrolle über die rapide Distribution verloren hatte und die Angriffe gegen Deutschland *Spill-Over*-Effekte waren.

7 VN Dokumente: S/2019/691; S/2022/668; S/RES/2397.

8 *Lazarus* und *Bluenoroff* sollen für komplexe finanziell motivierte Operationen und *Kimsuky* für politische und wirtschaftliche Spionage zuständig sein. Zudem wurde *Lazarus* für unterschiedliche disruptive Angriffe verantwortlich gemacht.

9 Universitäten in China sind u. a. das „Harbin Institute of Technology".

10 VN Dokumente: S/2019/691 S/2022/668; S/RES/2397.

Impressum

Der Autor

Lukas Joselewitsch ist im Referat OC 33 – Nationales IT-Lagezentrum, Analysen und Prognosen beim Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn tätig. Er hat *International War Studies* an der Universität Potsdam und dem University College studiert. Sein thematischer Fokus liegt auf Themen der Sicherheitspolitik, Diplomatie, Geopolitik, militärischen Auseinandersetzungen und Informationstechnik.

Konrad-Adenauer-Stiftung e. V.

Ferdinand Alexander Gehringer
Innere- und Cybersicherheit
Analyse und Beratung
T +49 30 / 26 996-3460
ferdinand.gehringer@kas.de

Postanschrift: Konrad-Adenauer-Stiftung, 10907 Berlin

Herausgeberin: Konrad-Adenauer-Stiftung e. V., 2024, Berlin
Gestaltung: yellow too, Pasiek Horntrich GbR
Satz: Janine Höhle, Konrad-Adenauer-Stiftung e. V.
Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-98574-215-8