https://globalsouth.co/2025/06/10/inside-the-cyber-operation-that-cracked-assads-leadership/

Eine Cyber-Operation brachte Assads Führungsriege zu Fall

Mit dem Übergang in eine neue Phase der hybriden Kriegsführung reicht es nicht mehr aus, den Himmel oder die Straßen zu kontrollieren. Man muss auch den Code kontrollieren.

10. Juni 2025 | Kevork Almassian

Was am 27. November 2024 in Aleppo geschah, war nicht nur ein Ereignis auf dem Schlachtfeld - es war ein politisches Erdbeben. Der schnelle Fall der Stadt und damit des Rückgrats der militärischen Präsenz des Assad-Regimes in Nordsyrien sandte Schockwellen durch die Region. Die Geschwindigkeit, mit der sich das Regime auflöste, erregte selbst bei seinen glühendsten Gegnern Aufsehen. Viele wussten, dass eine Militäroperation im Gange war, aber nur wenige verstanden den unsichtbaren Krieg, der sich hinter den Frontlinien abspielte.

Jetzt wissen wir es vielleicht.

Laut einer vom *New Lines Magazine* veröffentlichten Untersuchung war der Zusammenbruch der Syrischen Arabischen Armee in Aleppo nicht einfach das Ergebnis von Boden- oder Drohnenangriffen, sondern das Ergebnis einer verdeckten Cyber-Operation. Das Herzstück dieser Täuschung war nicht eine Rakete oder ein Panzer, sondern etwas viel Heimtückischeres: eine mobile Anwendung.

„Syria Trust For Development“: Ein trojanisches Pferd

Die unter dem Deckmantel einer humanitären Initiative gestartete App mit dem Namen STFD-686, eine Buchstabenfolge, die für Syria Trust for Development steht, erschien im Sommer 2024. Sie stand angeblich mit der First Lady Asma al-Assad in Verbindung und wurde als wohltätiges Programm vermarktet, das syrische Soldaten mit einem monatlichen Betrag von 400.000 syrischen Pfund – umgerechnet etwa 40 US-Dollar – unterstützen sollte.

Das Angebot war für viele Soldaten, die unter verzweifelten Bedingungen leben, unwiderstehlich.

Um die Zahlung zu beantragen, mussten die Nutzer eine Reihe persönlicher und scheinbar harmloser Angaben machen – Name, Geburtsdatum und Familiengröße. Doch dann kamen Anfragen nach sensibleren Informationen: militärischer Rang, Einheitsbezeichnung, Einsatzkoordinaten und Zugehörigkeit zur Befehlskette. Ein syrischer Softwareexperte, der mit der Operation vertraut war, sagte dem *New Lines Magazine*, dass die App so konzipiert war, dass sie genügend Daten extrahieren konnte, um die gesamte syrische Armeestruktur in Echtzeit abzubilden.

Das war aber noch nicht alles.

Die App erforderte eine Facebook-Integration und gewährte ihren Betreibern Zugriff auf soziale Graphen, private Nachrichten und Anmeldedaten. Nach der Installation wurde die Spionage-Software „Spy Max“ aktiviert, die ihren Betreibern uneingeschränkten Zugriff auf Telefonanrufe, Dateien, Fotos und sogar Live-Übertragungen von Kamera und Mikrofon des Geräts ermöglichte.

Kurz gesagt, jedes Telefon mit der App wurde zu einem mobilen Überwachungszentrum – und zwar aus den eigenen Reihen.

Gezielte Angriffe, unterbrochene Befehlsketten

Was dann kam, war klinisch und verheerend.

Die Julani-Truppen, die nun mit einer digitalen Karte der wichtigsten Schwachstellen des syrischen Militärs ausgestattet waren, gingen mit chirurgischer Präzision vor. Abgelegene Einheiten wurden isoliert und erhielten keinen Nachschub mehr. Hochrangige Offiziere mussten feststellen, dass ihre Befehle abgefangen oder widerrufen wurden. Ganze Verteidigungslinien in Aleppo brachen nicht wegen Personalmangels, sondern wegen strategischer Sabotage zusammen.

Und die ganze Zeit über hatten die Soldaten vor Ort keine Ahnung, dass sie selbst die Schlüssel übergeben hatten.

Es handelte sich nicht um einen Cyberangriff im herkömmlichen Sinne. Es handelte sich um psychologische Kriegsführung, die mit Hilfe von Technologie durchgeführt wurde und die Verzweiflung mit einem Versprechen auf Hilfe ausnutzte.

Wer steckte dahinter?

Das bleibt die Millionen-Dollar-Frage.

Die digitalen Fingerabdrücke sind undeutlich. Eine der Backend-Domänen der App wurde Berichten zufolge auf einem Server in den USA gehostet, was angesichts der langen Geschichte der Unterstützung von Julanis Gruppierungen durch Washington einen offensichtlichen Verdacht nahelegt. Die Beweise sind jedoch alles andere als schlüssig. Es könnte sich um eine absichtliche Falschmeldung gehandelt haben, um die Ermittler in die Irre zu führen und die Schuld abzuschieben.

Die wahrscheinlichere Realität? Es handelte sich um eine Operation mit mehreren Akteuren, bei der lokale Geheimdienstinformationen der Opposition, regionale Ressourcen und möglicherweise ausländisches Cyber-Know-how kombiniert wurden. Israel, die Türkei, Katar – allen ist die Cyber-Kriegsführung nicht fremd, und alle hatten ein strategisches Interesse daran, Damaskus zu schwächen.

Eine neue Ära der Kriegsführung

Wenn diese Operation etwas beweist, dann dies: Das Schlachtfeld ist nicht mehr nur ein physischer Raum. Die Cyber-Kriegsführung ist nicht mehr nur eine Ergänzung zur konventionellen militärischen Macht, sondern ein zentraler Bestandteil davon.

Erinnern wir uns an das Jahr 2020: Das vergessene Telefon eines syrischen Soldaten in einer russischen Pantsir-Luftabwehreinheit ermöglichte es Israel, das System zu triangulieren und per Luftangriff auszuschalten. Das war eine Warnung.

Was in Aleppo geschah, war die Erfüllung dieser Warnung.

> Die syrische Armee war nicht nur waffentechnisch unterlegen, sie wurde auch gehackt. Und da wir in eine neue Phase der hybriden Kriegsführung eintreten, reicht es nicht mehr aus, den Himmel oder die Straßen zu kontrollieren. Man muss auch den Code kontrollieren.

Im November 2024 hat der Programm-Code gewonnen.