Battlefield Digital Forensics: Ein Job für die Elite!

Bisherige forensische Fähigkeiten der Armee müssen ausgebaut werden. Sonderoperationskräfte übernehmen dabei eine tragende Rolle bei der digitalen Informationsbeschaffung. Es erhöht aber auch die Komplexität der Einsätze.

Oberstlt Philipp Leo, Chef Kommunikation Stab FUB, Partner Leo & Muhly Cyber Advisory
Fabian Muhly, wissenschaftlicher Mitarbeiter MILAK, Partner Leo & Muhly Cyber Advisory

Am 2. Mai 2011 wurde der Al-Qaida-Anführer Osama bin Laden durch amerikanische Sonderoperationskräfte in Pakistan getötet.

Bei diesem Einsatz wurden mehrere Computer, Mobiltelefone und unzählige weitere Datenträger in kürzester Zeit durch Gefechtsfeldforensiker sichergestellt. Nur wenige Stunden später wurde das Datenmaterial weltweit von staatlichen und ausgewählten privatwirtschaftlichen Analysten ausgewertet.

Der damalige CIA Direktor Leon Panetta kommentierte den Einsatz wie folgt: «Die auf den Computern der Terroristen gefundenen Informationen, haben sich jeweils als mindestens so wichtig erwiesen, wie die tatsächliche Tötung der Terroristen.»

Aktuelle Konflikte sind geprägt durch den umfassenden Einsatz von Informations- und Kommunikationstechnologien. Moderne Führungs- und Kommandoinfrastrukturen spiegeln diese Entwicklung wider. Es ist damit unausweichlich, dass Sonderoperationskräfte im Einsatz auf elektronische Kommunikationsmittel und Datenträger der Gegenseite stossen und somit eine fundamentale Rolle bei der Beschaffung nachrichtendienstlicher Informationen einnehmen können.

Die zusätzliche Herausforderung für Spezialkräfte besteht darin, Systeme und Datenträger im Einsatzraum aufzuspüren, sie auf Relevanz zu prüfen und so sicherzustellen, damit sie nachfolgend einer forensischen Analyse unterzogen und zeitnah nachrichtendienstlich verwertet werden können.

Diese Erweiterung des Aufgabenspektrums von Sonderoperationskräften durch die Gefechtsfeldforensik, erhöht die Komplexität von Einsätzen zusätzlich, kann aber auch einen beträchtlichen Informationsgewinn darstellen.

Aus nachrichtendienstlicher Sicht unterscheiden sich digitale Daten erheblich von anderen Informationsträgern und verlangen eine eigenständige Verarbeitung.

Die digitale Forensik deckt diesen Bereich ab. Sie umfasst nicht nur die Analyse von Desktop-Rechnern und mobilen Computern, sondern untersucht auch Mobiltelefone, Smartwatches, externe Datenträger, Netzwerke, Cloud-Speicher und andere Systeme.

Die Analyse von Protokollen, Zugangsdaten oder die Wiederherstellung gelöschter oder verschlüsselter Daten ist ebenfalls denkbar. Digitale Datenträger sind naturgemäss empfindlich und können durch unsachgemässe Handhabung verändert, beschädigt oder zerstört werden. Zudem kann die Gegenseite auch Schutzmassnahmen treffen, welche gefährdete Systeme durch eine automatische Zerstörung vor einer Untersuchung schützen sollen. Daher müssen spezialisierte Einsatzkräfte nicht nur in der Lage sein, potenzielle Quellen elektronischer Informationen, wie Computer, Netzwerkkomponenten oder Speichermedien, unter Zeitdruck zu identifizieren, sondern auch grundlegende Techniken der Informationssicherung beherrschen. Es gibt auch Bestrebungen, diese Einsatzkräfte durch Datenträgerspürhunde zu unterstützen. Diese besonders geschulten Spürhunde können auch versteckte Datenträger anhand des Geruches aufspüren.

Die kürzlich durch das VBS veröffentlichte Gesamtkonzeption Cyber stellt fest, dass die bisherigen forensischen Fähigkeiten der Armee nicht genügen und ausgebaut werden müssen. Es gilt die Gelegenheit zu nutzen, um diese Fähigkeiten nicht nur spezialisiert und isoliert in einem Fachbereich oder in einer Truppenformation aufzubauen, sondern diese im Verbund zwischen Kommando Spezialkräfte, Kommando Cyber und Nachrichtendiensten zu etablieren. In diesem Nachrichtenverbund kann die Gefechtsfeldforensik den kritischen Informationsvorsprung bedeuten.

Bild: NATO

Es ist unausweichlich, dass Sonderoperationskräfte im Einsatz auf elektronische Kommunikationsmittel und Datenträger der Gegenseite stossen.