Hacker leistete sensible Geheimdienstarbeit

18. September 2014

Thomas Knellwolf und Philippe Reichen, Tagesanzeiger

Die Strafakte offenbart es: Die Verdächtigen im Fall Giroud stehen dem schweizerischen Geheimdienst näher, als diesem lieb sein kann.

Bahnhofplatz Genf, 11. Juni 2014, 19.45 Uhr. Ein Agent des Nachrichtendiensts des Bundes (NDB) wird angehalten und abgeführt. Damit nimmt die Affäre um den Walliser Weinproduzenten Dominique Giroud eine spektakuläre Wende.

Bis zu jenem gewittrigen Abend drehte sich die Sache um mutmassliche Weinverschnitte und Steuerdelikte. Mit der Verhaftung des langjährigen Geheimdienstmitarbeiters hat sie den NDB erreicht. Sie wurde für den Dienst zu einer Belastung, die grösser ist als bislang bekannt. Dies zeigt sich in der Strafuntersuchung wegen des versuchten Hackerangriffs auf zwei Journalisten. Es konnten Akten zum Verfahren ausgewertet werden, das gegen ein sehr aktives Quartett läuft: den Agenten, Giroud, einen Genfer Privatdetektiv und einen Hacker.

Alle vier Beschuldigten bestreiten die Vorwürfe. Aber alle vier haben ausgesagt, sie hätten für den schweizerischen Geheimdienst gearbeitet, direkt oder indirekt. Der NDB hat dies mittlerweile der Genfer Generalstaatsanwaltschaft bestätigt - allerdings nur für den Agenten und den Privatdetektiv. Beim Hacker und schwächer bei Giroud deuten Indizien darauf hin, dass auch sie dem Staatsschutz zudienten.

Bei beiden geht der Nachrichtendienst auf Distanz. Besonders deutlich tut er dies beim Hacker, der mehrere Informatik-Start-ups gegründet und geleitet hatte und zuletzt im Kader des bundeseigenen Rüstungskonzerns Ruag tätig war. Der junge Genfer, so hat die NDB-Führung jüngst intern klargestellt, sei nie offiziell nachrichtendienstlich tätig geworden. Alles andere seien Schutzbehauptungen.

Das dreifache «Non» des NDB

Der Genfer Generalstaatsanwalt Olivier Jornot zeigt wenig Scheu, wenn es um Abklärungen zum Staatsschutz-Hintergrund seiner Beschuldigten geht. Er sandte am 23. Juni drei Seiten mit detaillierten Fragen zum Quartett nach Bern. Drei Tage später lag ein persönliches Antwortschreiben von Nachrichtendienst-Direktor Markus Seiler auf seinem Pult.

Beim Hacker lautet die Antwort dreimal «Non». «Nein», der Informatiker sei «nie als Mitarbeiter engagiert worden und er wurde nie als Quelle rekrutiert durch den NDB». «Nein», es sei nicht vorgesehen gewesen, dass der Hacker Informationen über die Aktivitäten des Agenten bekomme. «Nein», heisst es im Brief an den obersten Genfer Ermittler, auch zur Frage, ob der Hacker den Agenten bei der Arbeit habe beraten sollen.

Genau dies hat aber stattgefunden - und dies erst noch bei einem hochsensiblen Vorhaben. Bei der Hausdurchsuchung beim Privatdetektiv wurde eine Powerpoint-Präsentation sichergestellt.

Sie trägt den Vornamen des Agenten und zusätzlich den Titel «Bitcoin Feb 2014». Es handelte sich um ein Konzept, wie der NDB seine Quellen im Ausland künftig bezahlen könnte, ohne verdächtige Spuren zu hinterlassen. Die Idee: Eine anonyme Gesellschaft in der Schweiz sollte im Auftrag des Geheimdiensts Bitcoins kaufen. Die Internetwährung kann dann von einer Drittperson im Ausland in Bargeld umgewandelt werden. Die Vorteile: «Keine Kuriere, keine internationale Banktransaktion, solides Vertrags- und Zahlungsumfeld, Tarnung und ‹plausible deniability›, (…), beschränkte Kosten.»

Agent gibt alles zu

«Plausible deniability» lässt sich mit glaubhafter Bestreitbarkeit übersetzen. Verstanden wird darunter ein Konzept zum Vermeiden von Spuren. Im konkreten Fall könnte der Geheimdienst seine Auslandsquellen bezahlen, ohne dass Rückschlüsse auf die Herkunft des Geldes möglich wären. Flöge eine Zahlung trotzdem auf, liesse sich alles glaubhaft abstreiten.

In der Konfrontationseinvernahme gab der Agent nach anfänglichem Zögern zu, dass er den Hacker beauftragt hatte, das Konzept zu erarbeiten. Er habe diesen Auftrag und den Erhalt des Vorschlags beim NDB nicht protokolliert, obwohl er dies hätte tun müssen. «Ich habe jedoch», fügte der Agent hinzu, «darüber mit meinem direkten Vorgesetzten gesprochen.»

Geheimdienstchef Seiler bestätigt in seinem Schreiben an die Genfer Justiz, die «zusätzliche Mission» des Agenten, Möglichkeiten «anonymer Zahlungen ins Ausland abzuklären, um Quellen zu entlöhnen». In einem zentralen Punkt widerspricht der NDB-Direktor aber seinem Mitarbeiter. Dessen «Hierarchie» habe aber keine Kenntnisse davon gehabt, dass der Agent den Hacker konsultierte.

Um Quellen und Informanten zu schützen, gehört es zum Standardprozedere, dass innerhalb der Dienste nur wenige Mitarbeiter von geheimen und heiklen Aufträgen wissen. Die Tätigkeit des an der ETH Lausanne ausgebildeten Informatikers für den NDB könnte aber noch weitergegangen sein, sofern seine bei der Genfer Generalstaatsanwaltschaft gemachten Angaben korrekt sind. «Ich bin seit 2006 eine Quelle des Auslandgeheimdienstes», steht am Anfang des Protokolls der Aussage des Hackers. «Wenn sie während dieser Befragung eine gewisse Zurückhaltung spüren, ist es nicht, um Dinge zu verschleiern, sondern um das gebotene Schweigen einzuhalten.»

Der mysteriöse Norbert

Auf Nachfragen erzählte der Hacker dann aber von einem Führungsoffizier der schweizerischen Dienste, der sich «Norbert» genannt habe. Von 2006 bis 2009 hätten ein mittlerweile verstorbener Geschäftspartner und er für diesen Mann gearbeitet, dessen wahren Namen sie nicht gekannt hätten. «Es handelte sich dabei um extrem sensibles Hacking im Ausland», sagte der Hacker aus, ohne Details zu nennen. «Norberts» Telefonnummer sei auf seinem beschlagnahmten Handy gespeichert. Der NDB werde aber jede Verwicklung in die Operationen abstreiten.

In den Ermittlungsakten tauchten bislang aber keine weiteren Hinweise auf solche Aktionen auf. Gegenüber baz.ch/Newsnet wollten sich weder der Hacker noch dessen Anwalt zum allfälligen «extrem sensiblen Hacking» äussern. Der NDB verwies für alle Fragen an die Genfer Justiz. Doch auch dort ist dazu nichts Sachdienliches zu erfahren.

Und inwiefern war die ursprüngliche Hauptperson in der ganzen Affäre, Dominique Giroud, für den Nachrichtendienst aktiv? Der Weinproduzent hat am Tag nach seiner Verhaftung Aussagen

zu seiner Beziehung zum Agenten gemacht. Er sei mit ihm befreundet, seit er ihn Mitte der 90er-Jahre in einem Jugendlager in Schottland kennen gelernt habe. In jüngerer Zeit habe ihn sein Freund gefragt, ob er ihn bei seiner Berufstätigkeit unterstützen könne, «konkret als Mitarbeiter des NDB»: «Er hat mich gebeten, mein Beziehungsnetz einzusetzen. Das hat Anfang 2013 begonnen.» Mittlerweile bestreitet Giroud laut seinem Sprecher Marc Comina aber jede Aktivität für den Staatsschutz.

Girouds «interessantes Profil»

Dies steht nicht nur im Kontrast zu seinen eigenen Aussagen, sondern auch zu jenen des Agenten. «Es ist klar», steht in einem der Befragungsprotokolle, so gab der NDB-Mitarbeiter vielsagend zu Protokoll, «dass Dominique Giroud mit seinem Netzwerk ein sehr interessantes Profil hat.» Giroud habe ihm aber, so erinnert sich der Agent, deutlich gemacht, dass er bereits mit jemand anderem «bei uns» Kontakt hatte. Der Winzer habe ihm den Namen des Kollegen aus dem Dienst genannt, den er aber nicht im Gedächtnis behielt.

Tränengas und Pistole gefunden

Aus NDB-Sicht steht der Agent im Zentrum der ganzen Affäre. Bei ihm besteht der Verdacht, dass er seine Kompetenzen weiter überschritten hat. Bereits in jungen Jahren, noch als Genfer Spezialpolizist, hatte er im Skandal um den «Moscheespion» Claude Covassi eine kritisierte Rolle gespielt. Trotzdem war er kurz danach, im Jahr 2007, beim Bund untergekommen, wo er zuletzt mit dem Schutz des schweizerischen Finanzplatzes betraut war.

Noch im Morgengrauen vor seiner Verhaftung hatte der Agent eine Auslandmission angetreten. Kurz nach der Landung beorderten ihn sein Vorgesetzten jedoch zurück in die Schweiz. Wie geheissen, nahm der Staatsschützer den nächsten Flug zurück nach Zürich und den Zug nach Genf.

Der gebürtige Walliser musste geahnt haben, dass ihn keine harmlose Sache erwartete. Er war vorgewarnt. Seine Gattin hatte ihn per Handy wissen lassen, es habe unmittelbar nach seiner Abreise in ihrer Parterrewohnung nahe Freiburg eine Razzia gegeben. Sichergestellt wurden: ein Computer, ein iPad, benutzt von der ganzen sechsköpfigen Familie, mehrere Festplatten und Speichersticks, eine Tränengasgranate und eine Sig Sauer P229 mit Munition. Seine frühere Dienstpistole hatte der Agent privat erwerben können, als er noch selber bei der Genfer Polizei arbeitete. Den Behörden seines Wohnkantons hatte er sie allerdings nicht gemeldet. Zur Tränengasgranate sagte er kurz nach seiner Verhaftung aus: «Sie war in meiner Tasche geblieben.» Und: «Ich habe nie daran gedacht, sie zurückzugeben.»

Doch die Ermittler interessierten sich nicht allzu sehr für allfällige Verstösse gegen das Waffengesetz. Sie konzentrierten sich ganz auf die möglichen Verwicklungen des Agenten in Attacken auf die Computer zweier Enthüller von Girouds mutmasslichen Weinverschnitten und Steuerdelikten beim Westschweizer Fernsehen und bei der Zeitung «Le Temps». Der Geheimdienstmann gab zu, an Diskussionen über solche illegalen Aktionen beteiligt gewesen zu sei. Er beteuerte aber, sich deutlich dagegen ausgesprochen zu haben. Da es in den Aussagen der Verdächtigen starke Widersprüche gab, blieb das ganze Quartett zwei Wochen in Untersuchungshaft. Klarheit, wer die Cyberangriffe in Auftrag gab und wer sie - erfolglos - durchführte, besteht bis heute nicht.

Energiefirmen ausspioniert?

Allerdings gibt es nicht den geringsten Hinweis, dass die vier Beschuldigten auf Geheiss aus

Bern oder in offizieller Mission gehandelt haben. «Was den Fall Giroud betrifft», schreibt NDB-Sprecherin Isabelle Graber aktuell, «erinnere ich daran, dass der Genfer Generalstaatsanwalt bestätigt hat, dass der NDB nicht in diese Affäre verwickelt ist.» Und doch spielen Geheimdienstfragen in der Strafuntersuchung nach wie vor eine zentrale Rolle. Zwar sind auch der Genfer Justiz Grenzen gesetzt. So muss zum Beispiel bei abgehörten Telefongesprächen und abgefangenen SMS des Agenten zuerst geprüft werden, ob sie einen Bezug zum Strafverfahren haben, bevor sie ausgewertet werden.

Etwas Gewissheit herrscht über die Rolle des Detektivs: NDB-Direktor Seiler schreibt, der Mann sei ab Januar 2014 «offizielle Quelle» gewesen, «in Evaluationsphase». Er habe «nicht mehr als zwei Mandate bekommen, eines eine Recherche zu Personen aus Zentralasien, eines zur Ukraine». Der Detektiv selber sagte aus, er habe auch Aufträge zu Russland, Georgien und Armenien erhalten, oft zu Energiefragen.

WEF-Bedrohung analysiert

Verborgen blieb dem NDB, wie eng sein Agent, unzufrieden mit seiner Karriere, auf Eigeninitiative mit dem Detektiv und dem Hacker zusammenarbeitete. Das Trio schmiedete vergangenes Jahr Pläne für eine gemeinsame Überwachungsfirma. Die E-Mail-Adressen für alle drei waren bereits eingerichtet. Für das World Economic Forum erstellte man eine Bedrohungsanalyse. Doch das WEF verzichtete auf die Umsetzung des Sicherheitskonzepts.

Das Interesse des Agenten an der Selbstständigkeit schwand, als er beim NDB doch noch befördert wurde. Die Pläne für die Firmengründung verschwanden definitiv in der Schublade, als der Privatdetektiv im Februar 2014 unter Korruptionsverdacht verhaftet wurde. Wenige Monate zuvor hatte der Agent noch Startkapital fürs Unternehmen gesucht. In einer sichergestellten SMS schrieb er am 13. März 2013 dem Detektiv: «Ich habe vielleicht eine Finanzierungsart für unseren Laden gefunden.» Dies in der UBS-Filiale am Genfer Bahnhof, wo 13 Monate später seine Agententätigkeit ein abruptes Ende nahm.