Russland und die Internet-Propaganda

RUSSLAND UND DIE INTERNET-PROPAGANDA

Die US-Anklage von Februar 2018 gegen dreizehn russische Staatsbürger und drei Unternehmen im Zusammenhang mit dem Vorwurf der Einmischung in den amerikanischen Wahlkampf [1] wurde zwar von den Betroffenen sarkastisch kommentiert, jedoch sprachen auch auf russischer Seite genügend Indizien dafür, dass die in der US-Anklageschrift beschriebenen Vorgänge kein Konstrukt amerikanischen böswilligen Verhaltens war. Recherchen amerikanischer und russischer Medien in den vergangenen zweieinhalb Jahren haben ein relativ detailliertes Bild von dem ergeben, was gemeinhin als „Fabrik der Trolle“ bezeichnet wird.

So wird aufgezeigt, dass sich hinter einer harmlos scheinenden, privatwirtschaftlich organisierten Firma geheimdienstliche Aktivitäten, politische Absichten und Günstlingswirtschaft zu einem undurchsichtigen Konglomerat verbinden, von der der russische Staat stets beteuerte, damit überhaupt nichts zu tun zu haben. Die „Fabrik der Trolle“ heißt mit offiziellem Namen „Agentur für Internet-Recherchen“. Diese startete 2014 ihren Betrieb und war bis vor kurzem in einem unscheinbaren Bürogebäude in St. Petersburg untergebracht. Im Zwölf-Stunden-Schichtbetrieb arbeiteten bisher mehrere hundert Mitarbeiter in verschiedenen Abteilungen zur politischen Beeinflussung innerrussischer und ausländischer öffentlicher Debatten. Dabei ging es in erster Linie darum, Diskussionen durch die rege Beteiligung in den Leserkommentaren von Online-Medien und sozialen Netzwerken zu beeinflussen – eben zu „trollen“. Als sich das Verhältnis zwischen Russland und dem Westen im Zuge der russischen Einverleibung der Krim drastisch verschlechterte, lobten die Trolle in russischen sozialen Netzwerken und Presseerzeugnissen den starken Zusammenhalt der Gesellschaft gegen die äußere Gefahr.

Mittlerweile wird davon gesporchen, dass die besagte „Trollfabrik“ mit einem ganzen Medienkonglomerat verbunden ist. Die „Föderale Agentur für Nachrichten“ und eine Reihe von Internetmedien gehören dazu. Sie beliefert vielgelesene russische Nachrichtenportale mit Material – unter anderem auch aus dem Bürgerkriegsgeschehnissen in Syrien.

Der mutmaßliche „Besitzer“ der „Medienfabrik“ ist der undurchsichtige Gastro-Unternehmer Jewgeni Prigoschin, dem auch nachgesagt wird, dass er die Privatarmee Wagner mitfinanziert haben soll, die jüngst wegen erheblicher Verluste bei einem Zusammenstoss mit US-Truppen in Syrien in die Schlagzeilen kam. Prigoschin saß in den 1980er- Jahren wegen Raubes, Betrugs und Zuhälterei für neun Jahre im Straflager, bevor er mit einer Hotdog-Kette, russischem Fast-Food und einem sogar beim Präsidenten angesagten Petersburger Edelrestaurant in die obersten Ebenen der Macht Zugang fand und heute zahlreiche Behörden mit Essen beliefert. Das hat ihm den Spitznamen „Putins Koch“ beschert. Er ist einer der dreizehn angeklagten Russen und Besitzer der beschuldigten Unternehmen, bestritt aber hartnäckig jegliche Verbindungen zur besagten „Trollfabrik“.

Bezüglich der gescheiterten Bodenoffensive russischer Paramilitärs in Ostsyrien Anfang Februar 2018 hatte es offenbar Absprachen zwischen Regierungsstellen in Moskau und dem mutmaßlichen Drahtzieher der involvierten Truppe gegeben. So kündigte Prigoschin Ende Jänner 2018 gegenüber einem syrischen Minister offenbar die Offensive an und erklärte, er habe für die Operation der „Gruppe Wagner“ grünes Licht aus Moskau erhalten. Russland hatte offiziell jegliche Verbindung und Verantwortung für diesen paramilitärischen Einsatz bestritten. Bei den Angriffen der US-Luftwaffe auf die vorrückenden Kämpfer wurden offenbar Dutzende von russischen Söldnern getötet oder verwundet.

Mit der seit 2015 ins Leben gerufenen East Stratcom Task Force versucht die EU-Sonderabteilung – mit Schwerpunkt Osteuropa und Russland – die Flut an gegnerischer „Fake News“ und Desinformation einzudämmen.

Im ORF-Exklusivinterview vom Juni 2018 anlässlich seines Wien-Besuchs hatte der russische Präsident Wladimir Putin solche Bedenken der Europäer, bezüglich staatlich-russischer Hackerangriffe gegenüber dem Westen zerstreut. „Wir verfolgen nicht das Ziel, etwas oder jemanden in der EU zu spalten“, so Putin. Man sei stattdessen daran interessiert, dass die EU als wichtigster Handels- und Wirtschaftspartner „geeint ist und floriert“.

Bei allem negativen Schlaglicht auf Russlands Aktivitäten in diesem Bereich dürfe aber nicht darüber hinweggesehen werden, dass derzeit entsprechend defensive wie offensive Cyberwar-Strategien [2] mit Hochdruck von allen relevanten Großmächten [3] entwickelt werden. (Auch Österreich hat zum Schutz kritischer Infrastruktur [4] eine dementsprechende Strategie ins Leben gerufen.)
Weiterführende LINKS:

Putins strategische Ziele. In: ÖMZ 1/2017

Walter J. Unger/Sigmar Stadlmeier/Andreas Troll, Cyber Defence - eine nationale Herausforderung (Teil 1) – ÖMZ 5/2014

Walter J. Unger, Cyber Defence - eine nationale Herausforderung

Netzpropaganda - Wie ich einmal Putins Trolle traf. In: SPIEGEL-Online v. 17.12.2017

Hip, jung und gewissenlos – das sind Putins Trolle. In: DIE WELT-Online v. 29.5.2016

EU-Kommission über „Fake News“

EUvsdisinfo

Wie sich die EU und die Nato auf hybride Angriffe vorbereiten. In: NZZ-Online v. 18.12.2018

Russland probt den ersten hybriden Weltkrieg | NZZ

Russian Cyber Attacks: Is the West Vulnerable?

HACkS, LEAkS ANd dISRUPTIONS | RUSSIAN CYBER - CHAILLOT PAPERS

Austrian Cyber Security Strategy - Bundeskanzleramt Österreich

Feichtinger kompakt: Verteidigung ist neu zu denken

In Cyberwar, There are No Rules – Foreign Policy

Cybersecurity and Cyberpower - oiip

National Cyber Strategy - The White House

Russia’s Cyber Strategy

Anmerkungen:

[1] Bryan Wilder/Yevgeniy Vorobeychik, „Controlling Elections through Social Influence“. In: arXiv:1711.08615v1 (cs.MA) 23. Nov 2017.

[2] Anika Torruella, „Hunting for a signal in the noise“. In: IHS Jane’s Internationale Defence Review 9/2016, S. 60-65.

[3] Vgl. dazu etwa:

Christopher A. Bartos, „Cyber Weapons Are Not Created Equal“. In: U.S. Naval Institute, Proceedings Magazine - June 2016, Vol. 142/6/1, 360, S. 30-33.

John Antal, „The Cyber Arms Race The US and NATO Playing Catch-up“. In: MILITARY TECHNOLOGY 11/2017, S. 22-25.

Alex Gorka, „US Responsible for Cyberspace Becoming a War Domain Instead of an Area of Cooperation“. In: Strategic Culture Foundation-Online v. 3.10.2018.

„NATO Coordinates Information War on Russia“ - Strategic Culture Foundation-Online v. 5.10.2018.

[4] Vgl: Sorin Dumitru Ducaru, „The Security of Critical Energy Infrastructure in the Age of Multiple Attack Vectors: NATO's Multi-Faceted Approach“. In: Europolity 1/2017, S. 5-19.