Sozialdemokratische Partei der Schweiz / Parti Socialiste Suisse
Zentralsekretariat / Secrétariat central
Theaterplatz 4, 3011 Bern
Tel. 031 329 69 69 / www.spschweiz.ch / www.pssuisse.ch

# Fachkommission für Frieden und Sicherheit / Einladung – Invitation

Liebe Mitglieder der Fachkommission für Frieden und Sicherheit

Ich lade Euch im Namen unserer Präsidentin NR Priska Seiler herzlich zur nächsten Sitzung der Fachkommission für Frieden und Sicherheit der SP Schweiz ein. Mit eingeladen sind die Mitglieder der Fachkommission für Verkehr und Kommunikation und der AG Medienpolitik. Wir treffen uns am

**Dienstag, 12. Dezember 2017, 18.15 – 20.15 Uhr**
**Bern, Bundeshaus, Zimmer 8**
**Achtung:** Bitte diese Einladung und einen Pass oder ID mitbringen,
Eingang Bundesterrasse benutzen und dort vorweisen

## Traktanden

1. Begrüssung, Traktandenliste, Protokoll der letzten Sitzung (bereits verschickt)

## 2. Desinformation durch fremde Mächte: Wie unsere Demokratie gegen Fake news und automatisierte „Social Bots" schützen? Wie unsere Sicherheit im Informationskrieg gewährleisten?

Einführung:

Adrian Rauchfleisch, Universität Zürich, Wissenschaftlicher Assistent am Institut für Publizistikwissenschaft und Medienforschung, Abteilung Wissenschafts-, Krisen- & Risikokommunikation, Mitgründer von ZIPAR (machte u.a. Studie zur Rolle gefälschter Online-Kommentare im Auftrag politischer Akteure)

David Rechsteiner, Universität St. Gallen, Lehrbeauftragter für Bundesstaatsrecht, Ko-Autor „Social Bots und Meinungsbildung in der Demokratie"

Christian Catrina, VBS, stellvertretender Generalsekretär VBS, Chef Sicherheitspolitik

Die gezielte Lancierung von „Fake News" und deren massenhafte Verbreitung mittels automatisierter „Social Bots" hat in den Medien teilweise heftige Diskussionen ausgelöst. Die russische Einflussnahme auf die Präsidentschaftswahlen in den USA befeuerte diese Debatte zusätzlich, erreichte doch allein die (faktenferne) russisch finanzierte Facebook-Werbung über 120 Millionen US-Wähler und -Wählerinnen.

Das Thema geht weit über Russland und die USA hinaus. Laut Freedomhouse übten Online-Manipulationen und Desinformation in mindestens 18 Staaten starken Einfluss auf die Wahlen aus. Von aussen gelenkte Desinformationskampagnen zielen nicht zuletzt auf Staaten, welche die Meinungsäusserungsfreiheit sehr hoch bewerten und deshalb bisher eine weitergehende Regulierung der Social Media ablehnten. Am anderen Ende des Spektrums stehen jene 25 autoritären Staaten, die das Internet regelmässig blockieren sowie jene rund 30 Staaten, die es selber massiv für Staatspropaganda nutzen. Das Magazin vom 2. Sept. 2017 bezeichnete diese Aktivitäten unter dem Titel „Stell Dir vor, es ist Krieg, und keiner merkt's" summarisch als „Informationskrieg". Das geht wohl etwas gar weit. Ohne Zweifel ist der Übergang zwischen normaler Lage und Krieg aber vielerorts fliessend geworden und sind gerade auf dem Gebiete der Desinformation hybride Formen der Konfliktaustragung üblich.

Dennoch sollten die medienpolitische und die sicherheitspolitische Dimension von Desinformation und Informationskrieg wohl auseinandergehalten werden.

Medienpolitisch wird die Frage intensiv diskutiert, ob der Staat regulierend in die Social Media eingreifen soll, um die Demokratie zu schützen, die grundlegend auf dem Konzept der Öffentlichkeit und der Unterscheidbarkeit von Tatsachen, Meinungen und Lügen beruht. Der Bundesrat hat diese Frage letztmals am 10. Mai 2017 in seinem Nachfolgebericht über die „Rechtliche Basis für Social Media" verneint. Der Bundesrat geht dort in den Kapiteln 2.4.3 und 2.4.4 eingehend auf „Fake News" und „Social Bots" ein und hält einerseits fest, es seien die dadurch „verursachten Probleme als ernsthaft" einzuschätzen, es genüge aber vorerst, „durch stetige Beobachtung des Phänomens zu untersuchen, ob die bestehenden Massnahmen zusammen mit den Instrumenten der Selbstregulierung genügen oder ob zusätzlich

ein staatliches Eingreifen notwendig ist.“ (S. 15). Die Schweiz hält hier also bisher an ihrer äusserst liberalen Haltung fest. Viele andere Länder gehen hier deutlich weiter. Mögliche Massnahmen sind:

1. Entlarvung: Staatliche Subventionen an NGO wie die estnische NGO Propastop, welche versucht, Fake News und andere in den Medien verbreitete Lügen zu entlarven und richtig zu stellen.
2. Transparenzvorschriften: Die Verpflichtung von Facebook, Twitter und anderen Social Media Plattformen, den Auftraggeber von politischer Werbung offen zu legen und – als Steigerung – generell eine eineindeutige Identifikation der sich in Social Media äussernden Personen zu gewährleisten.
3. Die Unterstellung der Social Media unter das Radio- und Fernsehgesetz RTVG, das in Art. 4 Abs. 2 fordert, dass Sendungen mit Informationsgehalt „Tatsachen und Ereignisse sachgerecht darstellen, so dass sich das Publikum eine eigene Meinung bilden kann“.
4. Die Unterstellung der Social Media unter das Medienrecht, namentlich das Recht auf Richtigstellung (Art. 74 StPO) und das Gegendarstellungsrecht (Art. 28g ZGB folgende)[1].
5. Verbot von Hasspropaganda in Social Media: Der Deutsche Bundestag hat im Zuge der Terrorismusdebatte im Sommer 2017 das hoch umstrittene Netzwerkdurchsetzungsgesetz verabschiedet, das Plattformbetreiber verpflichtet, „offensichtlich strafbare Inhalte“ innerhalb von 24 Stunden zu löschen.

Sicherheitspolitisch wird diese Debatte sozusagen als dritte Dimension der Cyber-Diskussion geführt, die bisher in der Schweiz mehrheitlich auf (1) Cyberkrieg und (2) Cyberkriminalität (inkl. Cyber-Vandalismus) fokussiert war. Die hier interessierende dritte Dimension – (3) Desinformation (als medienpolitisches Thema im Alltag) und Informationskrieg (als sicherheitspolitisches Thema als Vorstufe einer massiven Konflikteskalation) – tauchte bisher kaum auf dem Radar der Sicherheitspolitik auf. Denn das aktuelle Ausmass von Desinformation z. Bsp. durch russische Aktivitäten auf Facebook, Twitter, Internetseiten (wie Sputniknews) oder in den Kommentarspalten von Newsportalen wird als sicherheitspolitisch irrelevant eingeschätzt und das in einer unbekannten Zukunft vorhandene Risiko eines ausgewachsenen Informationskrieges – die Eroberung des Informationsraumes als ultimatives Kriegsziel: die Weltsicht des Gegners zu kontrollieren – offenbar als tragbar. So geht der sicherheitspolitische Bericht des Bundesrates vom 24. August 2016 zwar im analytischen Kapitel 2.1.5 „Weiterentwicklung des Konfliktbildes“ zwar eingehend auf „Propaganda und Desinformation“ ein und misst solchen Informationsoperationen in der „hybriden Kriegführung“ „eine zentrale Rolle“ zu. Wenn wir jedoch im SIPOL Vorschläge suchen, wie die Schweiz auf diese Herausforderung reagieren soll, so bleibt er seltsam vage: Es sei erforderlich, „dass die Behörden die Möglichkeit von gegnerischen Informationsoperationen berücksichtigen und die Bedeutung einer aktiven und objektiven Information erkennen.“ „Berücksichtigen“ und „erkennen“ bedeutet ganz offensichtlich, dass keine Planungen bestehen, Fähigkeiten zu eigenen Informationsoperationen aufzubauen. Ganz in dieser Logik enthält das Reglement „Operative Führung“ war die Kapitelüberschrift „Informationsoperationen“. Dort findet sich aber nichts als der lapidare Hinweis, dieser Bereich befinde sich „zur Zeit“ noch „in Bearbeitung“ – ohne erkennbaren Zeithorizont.

Die Europäische Union sowie die NATO sind hier deutlich weiter. Die EU hat am 13. September 2017 ein umfassendes „Reformpaket zur Cybersicherheit“ veröffentlicht, das an die Initiative des Europäischen Rates zur Errichtung eines digitalen Binnenmarktes anknüpft und in einer Mitteilung der Kommission namentlich einen deutlichen Ausbau des Strategischen Kommunikationsteams Ost (East StratCom Task Force) im Europäischen Auswärtigen Dienst EAD empfiehlt (dazu auch Zeit-Online).

Die NATO hat ihrerseits in Tallinn ein Zentrum für Strategische Kommunikation (StratCom) aufgebaut, das der Koordination und dem angemessenen Gebrauch der NATO Kommunikationsaktivitäten und -fähigkeiten gewidmet ist. StratCom unterstützt ferner die Politikformulierung und das Führen von Operationen, so mit der Studie von Keir Giles über die zukünftige Informationskriegführung. Laut Jahresbericht 2016 über die Teilnahme der Schweiz an der Partnerschaft für den Frieden unterhält die Schweiz zwar Kontakte zum *Cooperative Cyber Defence Center of Excellence* der Nato in Tallinn. Weder hier noch im „Aktionsplan Cyber-Defence“ des VBS vom 9. November 2017 finden sich aber Hinweise auf den Aufbau einer eigenen Strategischen Kommunikationsfähigkeit. Das Dokument geht auf Cyber-Defence und Cyber-Kriminalität und -Vandalismus ein, nicht aber auf Desinformation und Propaganda. Gegen gezielte Informationsoperationen scheint die Schweiz nach wie vor nichts vorgekehrt zu haben.

## 3. Nächste Sitzung

Jeweils am dritten Dienstag der Session von 18.15 – 20.15 Uhr. Nächstes Mal: **13. März 2018**

Mit besten Grüssen Peter Hug

---

[1] Siehe auch die Empfehlung Rec(2004)16 des Ministerkomitees des Europarats vom 15.12.2004 über das Recht auf Gegendarstellung in der neuen Medienumgebung und die Entschliessung 2066 (2015) der Parlamentarische Versammlung des Europarates über die Verantwortung und Ethik der Medien im sich verändernden Medienumfeld.