Informationskriegsführung

Cybersecurity – Herausforderungen für die politische Schweiz

Stand der Dinge

Information Warfare ist eine zunehmende Bedrohung, insbesondere für westliche Demokratien, von dem alle gesellschaftlichen Akteure betroffen sind. In diesem Kapitel identifizieren wir insbesondere den Handlungsbedarf in Hinblick auf staatliche Akteure, um deren Rolle und Aufgabe einzuordnen und prioritäre Handlungsfelder hervorzuheben.

Das Thema der Informationskriegführung (engl.: «Information Warfare») hat eine längere Tradition, sowohl international wie auch in der Schweiz. Der Oberbegriff hat in den späten 90er Jahren bis ca. 2010 alle relevanten Themen, von der Kriegführung im Cyberraum bis hin zu Propaganda, Desinformation und psychologischer Kriegsführung, umfasst. Das Thema wurde sowohl im Rahmen der Strategischen Führungsübung 97 (SFÜ) wie auch innerhalb der Schweizer Armee konzeptionell im Rahmen der Konzeptionsstudie Informationsoperationen (KS IO) aufgearbeitet. Die heutige Verwendung des Begriffs bezieht sich zunehmend auf die Beeinflussung der öffentlichen Meinung mittels semantischer Methoden, wobei die technologischen Aspekte eine der treibenden Kräfte für die Umsetzung dieser Operationen darstellen.

In den 90er Jahren haben verschiedene Organisationen und Forscher auf mögliche Entwicklungen im Rahmen der Verwendung digitaler Technik für die Produktion und Verbreitung von verschiedentlich manipulierten Informationen aufmerksam gemacht. Dies ist aber erst mit dem Aufkommen der sozialen Medien und der breiteren Verfügbarkeit von Machine-/Deep Learning Technologien zu erschwinglichen Preisen relevant und real geworden.

Empfehlungen

1. Entwicklung staatlicher Fähigkeiten zur Erkennung und Zuordnung von Einflussoperationen. Diese sollten alle Ebenen des Staates (Bund, Kanton, Gemeinde) einbeziehen und auf Bundesebene koordiniert werden.
2. Rechtliche Grundlagen überprüfen, um Reaktionen auf Beeinflussungsoperationen zu ermöglichen und klare Richtlinien für mögliche Verteidigungsoptionen oder Gegenangriffe festlegen.
3. Mit den nationalen Medien zusammenarbeiten, um Desinformationen zu entlarven und die Bevölkerung für das Problem zu sensibilisieren.
4. Vereinbarungen treffen mit wichtigen sozialen Plattformen, die in der Schweiz als Unterstützung zur Bekämpfung von Social Media Einflussoperationen genutzt werden können.
5. Schaffung eines Alarmierungssystems bei laufenden Angriffen (wie bei SwissAlert oder als Teil davon).
6. Politische Koordination mit der Europäischen Union zur Bekämpfung von Social Media-Einflussoperationen, z.B. im Zusammenspiel mit Social Media-Plattformen.
7. Social-Media-Kompetenz und Bewusstsein für digitale Risiken in Bildungsprogramme integrieren.
8. Unterstützung von Fact-Checking-Initiativen, die speziell auf den Schweizer Kontext abzielen.

Der Einsatz von Algorithmen der künstlichen Intelligenz, Automatisierung und grossen Datenmengen im Web und in den sozialen Medien verändert den Umfang, die Reichweite und die Präzision, wie computergestützte Propagandakampagnen zur Manipulation der öffentlichen Meinung eingesetzt werden können. Heute ist es möglich, Inhalte automatisch oder halbautomatisch zu produzieren, sie in Text, Sprache und Bilder umzuwandeln und sie einer breiten und auf bestimmte Zielgruppen fokussierten Masse von Menschen in kürzester Zeit und ohne nennenswerte Kostenfolge zugänglich zu machen. Die Natur der sozialen Medien macht sie besonders anfällig für Angriffe. Filterblasen und Echokammern können erzeugt und verstärkt werden; Memes, Fotos und Videos können zur Verbreitung von Informationen genutzt werden, ohne dass eine Überprüfung der Quelle möglich ist; Gemeinschaften können angegriffen werden, indem gefährdete persönliche Profile oder einflussreiche Netzwerkknoten identifiziert werden.

Social Media werden von Regierungen und politischen Parteien manipuliert. Gemäss einer Studie des Oxford Internet Institutes[1] liegt Evidenz für organisierte Social-Media-Manipulationskampagnen durch Cybertruppen oder politische Parteien für 70 Länder im Jahr 2019 vor, gegenüber 48 Ländern im Jahr 2018 und 28 Ländern im Jahr 2017. In autoritären Staaten wird Social-Media-Manipulation als Instrument zur Kontrolle der eigenen Bevölkerung eingesetzt. Demokratische Staaten sind Ziel von Beeinflussungsoperationen, die von einer Handvoll Akteuren ausgeführt werden, darunter (gemäss Beweislage) China, Indien, Iran, Pakistan, Russland, Saudi-Arabien und Venezuela. Die Grösse der Cybertruppen in China wird heute auf 300’000 bis 2 Millionen Personen geschätzt. Darüber hinaus arbeiten die Cybertruppen oft mit der Privatwirtschaft, zivilgesellschaftlichen Organisationen, Internet-Subkulturen, Jugendgruppen, Hackerkollektiven, Randbewegungen, Einflussnehmern der sozialen Medien und Freiwilligen zusammen, die ihre Sache ideologisch unterstützen.

Es gibt eine Vielzahl von Techniken zur Durchführung von Beeinflussungsoperationen, darunter Desinformation, Social Hacking, betrügerische Identitäten, Bots und Trolling. All diesen Techniken ist gemeinsam, dass dadurch politische Vorgänge (z.B. Wahlen) beeinflusst oder gar Revolten und Revolutionen ins Rollen gebracht werden. Das destabilisierende Potential dieser Art der Kriegführung basiert auf einem tieferen Verständnis menschlicher Entscheidungsprozesse und der Dynamik von Massenphänomenen. Diese Aspekte können wiederum immer einfacher dank neuer Technik und Algorithmen simuliert werden.

.

Herausforderungen

Operationen, die auf staatlicher Ebene versuchen Einfluss zu nehmen, können die öffentliche Meinung in einem Land zugunsten des Angreifers verändern. Daher sind Demokratien, in denen der politische Entscheidungsprozess stark in der öffentlichen Meinung verwurzelt ist, besonders anfällig für diese Art von Angriffen.

Beeinflussungsoperationen sind aus einer Reihe von Gründen für den Angreifer attraktiv:

1. sie sind relativ kostengünstig durchzuführen.
2. sie sind schwer zuzuordnen, und das Risiko einer Eskalation ist begrenzt.
3. sie ermöglichen die Instrumentalisierung der Benutzer in grossem Massstab.
4. sie können allein oder in Kombination mit anderen Formen der Kriegsführung (traditionell, wirtschaftlich) eingesetzt werden.

Andererseits ist es schwierig, die Effizienz und die Auswirkungen von Beeinflussungsoperationen zu bestimmen. Sie laufen zudem Gefahr, für den Angreifer ausser Kontrolle zu geraten. Dennoch kann

[11] https://comprop.oii.ox.ac.uk/research/cybertroops2019/

bei mehreren Ereignissen der letzten Zeit, insbesondere bei den Wahlen in den USA, in UK und in Frankreich, davon ausgegangen werden, dass es zu Änderungen der öffentlichen Meinung gekommen ist. Offen bleibt, ob diese Änderungen schliesslich entscheidend waren.

Ebenfalls eine offene Frage bleibt, ob die Schweiz bereits das Ziel ausgeklügelter Beeinflussungsoperationen war. Es gibt Anzeichen dafür, dass diese bei bestimmten politischen Themen aufgetreten sind (z.B. Billag-Abstimmung, 5G-Kontroverse).

Handlungsbedarf

Die offizielle Schweiz stellt sich auf den Standpunkt, dass die aktive Verwendung von manipulierter Information für die Erreichung von politischen Zielen für einen demokratischen Staat kein adäquates Mittel ist. Umso wichtiger ist es, folgende Aktionen als Antwort auf die Bedrohung durch Information Warfare umzusetzen (vgl. dazu auch den EU action plan):

1. Fähigkeiten zur Erkennung, Analyse und Attribuierung von Beeinflussungsoperationen: Aktionen durch Dritte im eigenen Interessenraum sind frühzeitig zu erkennen, zu analysieren und zu attribuieren. Hierfür unerlässlich ist Zugang zu relevanten Daten und Datenanalyse-Werkzeugen sowie zu menschlichen Analyse Fähigkeiten. Sie sollten Teil der Fähigkeiten der staatlichen Behörden sein, in Zusammenarbeit mit privaten Akteuren und in internationaler Zusammenarbeit. Die ständige Analyse der verwendeten semantischen und technologischen Ansätze hilft dabei, die Frühwarnung aufzubauen und sicherzustellen. Nicht zu vernachlässigen ist der Aspekt der Zeitverhältnisse: verbreitete Falschinformationen können lange unentdeckt im Hintergrund zirkulieren und auf einmal z.B. gewaltsame Aktionen von vielen Menschen verursachen.
2. Reaktion auf entdeckte Beeinflussungsoperationen: Sobald sie entdeckt wurden, werden Reaktionen von den staatlichen Behörden auf der Grundlage der verfügbaren gesetzlichen Grundlage umgesetzt. Reaktionen können Warnsysteme, faktenbasierte Kommunikation in den Medien oder die Begrenzung der Kapazitäten des Angreifers erfordern. Es geht dabei auch darum, der eigenen Bevölkerung den Zugang zu verlässlichen Informationen und Fakten zu ermöglichen. Dieser Prozess muss transparent und nachvollziehbar bleiben, damit die verbreiteten Informationen auch unabhängig verifiziert werden können.
3. Interaktion zwischen staatlichen Behörden und dem Privatsektor: Um soziale Manipulationen aufzudecken oder darauf zu reagieren, sind staatliche Akteure auf die Zusammenarbeit mit dem Privatsektor angewiesen, insbesondere mit den Betreibern von Social-Media-Plattformen und den Medien. Die Zusammenarbeit kann in besonders schweren Fällen den Zugang zu relevanten Daten, die Schliessung verdächtiger Konten, die Entfernung falscher Informationen oder die Information der Bevölkerung über solche Angriffe und die Berichtigung von Desinformationen betreffen.
4. Erhöhung der gesellschaftlichen Widerstandsfähigkeit: Da soziale Manipulation auf den allgemeinen Bürger abzielt, ist es von entscheidender Bedeutung, die Gesellschaft für diese Phänomene zu sensibilisieren. Konkrete Massnahmen umfassen die Aufklärung von Menschen aller Altersgruppen darüber, wie sie solche Angriffe erkennen und auf sie reagieren können, sowie den Einbezug der Allgemeinbevölkerung in defensive Aktivitäten, wie z.B. Faktenüberprüfung.

Generell gilt, dass Grundrechte wie die freie Meinungsäusserung für unsere Gesellschaft fundamental und stark darin verankert sind – somit sind Einschränkungen beim Zugang zu Informationen nur als Ultima Ratio bei besonders schweren Fällen mit kriminellem Charakter gerechtfertigt. Umso wichtiger ist aber auch hier eine zeitgerechte Antwort in Form von Information.

Referenzen

Action Plan against Disinformation, Joint Communication to The European Parliament, The European Council, The Council, The European Economic and Social Committee And The Committee of The Regions, Brussels, 5.12.2018 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019JC0012

Cyber Influence Operations: An Overview and Comparative Analysis, Center for Security Studies (CSS), ETH Zürich, Zürich, October 2019 https://css.ethz.ch/en/services/digital-library/publications/publication.html/c4ec0cea-62d0-4d1d-aed2-5f6103d89f93

The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation. Working Paper Oxford, 2.2019 https://comprop.oii.ox.ac.uk/research/cybertroops2019/

Appendix

Erklärung einiger häufiger Formen des Information Warfare

- **Desinformation**: Verbreitung falscher oder unvollständiger Information mti der Absicht zu täuschen.
- **Social Hacking**: Nutzung sozio-kognitiver Eigenschaften des menschlichen Geistes, insbesondere Stammesdenken und Hang zur Konformität.
- **Betrügerische Identitäten**: Nutzung legitimer Identitäten durch illegitime Akteure.
- **Bots**: Automatisierte Computersoftware zur Manipulation von online Plattformen.
- **Trolls**: Nutzer oder Bots, die gezielt Nutzer attackieren, beleidigen oder angreifen.

Kontakt

Nicole Wettstein
Leiterin Schwerpunktprogramm Cybersecurity
+41 44 226 50 13

https://www.satw.ch/cybersecurity-herausforderungen

Impressum
Schweizerische Akademie der Technischen Wissenschaften SATW
Expertenbeiträge
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Verwaltungsrat und Berater | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Redaktion und Grafik
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
September 2020