Bild: Romolo Tavani/Shutterstock.com

Informationskriegsführung zu Beginn des Informationszeitalters

Autor:
Tim Sweijs

Zusammenfassung

Zu Beginn des Informationszeitalters deutet alles auf die Verbreitung und Weiterentwicklung von Werkzeugen bzw. die Verfeinerung von Taktiken hin, die bei Desinformationskampagnen verwendet werden. 5G wird die Geschwindigkeit der Informationsflüsse drastisch erhöhen, die Verbreitung von Augmented-Reality- und Virtual-Reality-Applikationen vorantreiben sowie die Art, wie Menschen Informationen aufnehmen und die soziale und materielle Realität erleben, grundlegend verändern. Dies wird neue Möglichkeiten für den Informationskrieg eröffnen. Wirksame Gegenmaßnahmen sind Bildung der Bevölkerung, bessere Schutzmaßnahmen durch Regulierung des Privatsektors und der Aufbau einer strategischen Abschreckung.

Strategische Innovationen

Die massive digitale Vernetzung unserer Gesellschaften in den beiden vergangenen Jahrzehnten hat für Wirtschaftswachstum und sozialen Umgang neue Möglichkeiten eröffnet. Dadurch sind auch neue Tools entstanden, mit denen Akteure in Konflikten ihren Gegnern Schaden zufügen können. Für diese Akteure stellen oligopolistische Social-Media-Plattformen global agierender E-Tech-Unternehmen, die von den Regierungen weitgehend unreguliert blieben, eine einfache Möglichkeit dar, um gesellschaftliche Diskurse zu manipulieren und zu verzerren. Strategisch innovative Akteure, insbesondere Russland, erkannten schneller als andere das enorme destruktive Potenzial der Vernetzung moderner Gesellschaften und haben damit begonnen, aktiv die Inhalte von Informationsflüssen in westlichen Gesellschaften zu manipulieren. Wir erleben die Neuauflage der Informationskriegsführung im Stil des 21. Jahrhunderts.

Taktik und Ziele

In Trollfabriken wurden Cyber-Einheiten eingerichtet und mit virtuellen Werkzeugen ausgestattet, die im Vergleich zur herkömmlichen Ausrüstung für Verteidigungszwecke relativ wenig kosten. Diese Einheiten begannen mit der massenhaften Schaffung gefälschter Identitäten auf populären Social-Media-Plattformen, um Falschinformationen zu verbreiten und Kampagnen zu beeinflussen. Sie entwickelten ein differenziertes Verständnis dafür, wie Informationen durch Netzwerke wandern und wie proprietäre Algorithmen von Social-Media-Plattformen genutzt werden können. Sie verwenden unterschiedliche Taktiken, um gesellschaftliche Diskurse zu verzerren, etwa durch Einbringung von Falschinformationen in verschiedene Nischennetzwerke oder durch Überschwemmung von Plattformen mit bestimmten Meinungen, um gewisse Stimmen zu übertönen und bestimmte Meinungen stärker ins Rampenlicht rückten. Ihr Ziel ist es, Zwietracht zu stiften, die Polarisierung zu verstärken sowie das Vertrauen und den Zusammenhalt der Gesellschaft zu untergraben.

Bedrohungsbewusstsein

Die ausführliche Dokumentierung der russischen Einmischungsversuche, zunächst in den USA und dann bei verschiedenen Wahlen in Europa, hat das Ausmaß dieser Informationskampagnen deutlich gemacht und zuerst eine Schockstarre ausgelöst. Die europäische Gegenreaktion folgte einem typischen Muster: zuerst Skepsis und Verleugnung, dann Erstaunen, aber auch Erkennen der Bedrohung, und schließlich der übliche Schnellschuss. Ein Beispiel dafür war eine ohne genaue Recherchen geführte schwarze Liste von Medien, die Artikel verbreiteten, welche im Zusammenhang mit prorussischen Perspektiven als Provider von Fake News gelten konnten. Schließlich begannen europäische Entscheidungsträger differenzierter über Maßnahmen gegen das neue Phänomen der Informationskampagnen zu reflektieren. Auch die Rolle der riesigen Social-Media-Plattformen wurde genauer untersucht, insbesondere nachdem bekannt geworden war, dass Cambridge Analytica mit Daten von Millionen von nichtsahnenden Facebook-Nutzern psychologisches Profiling durchgeführt hatte.

Die erste Reaktion

Etwa ab 2017 begannen die europäischen Regierungen, Maßnahmen zum Schutz ihrer demokratischen Diskurse entlang eines präventiv-reaktiv-proaktiven Politspektrums umzusetzen. Die Regierungen stellten Geld für die Vermittlung von Medienkompetenz in Grund- und Mittelschulen bereit. Sie setzten Beschränkungen für die ausländische Eigentümerschaft von Medien. Um die manipulative Nutzung von sozialen Medien zu verfolgen und aufzudecken, wurden Kooperationen mit Forschungseinrichtungen oder teilweise unabhängigen Regulierungsbehörden aufgebaut. Traditionelle Medien intensivierten ihre Berichterstattung und schärften das Bewusstsein der Öffentlichkeit für ausländische Einflusskampagnen. Europäische Regierungen verstärkten ihre strategischen Kommunikationsfähigkeiten, um viralen Narrativen entgegenzuwirken. Auch für jene hinter den sozialen Medien stehenden Unternehmen, die sich bis zu diesem Zeitpunkt ihres ursprünglichen Anspruchs, neutrale Akteure zu sein, entledigt

hatten, wurden Regelungen erarbeitet. Diese Unternehmen forderten aktiv Leitlinien und Vorschriften und unternahmen größere Anstrengungen, sich mit der bewussten – und oft automatisierten – Manipulation der auf ihren eigenen Plattformen zirkulierenden Informationen zu befassen.

Der Beginn einer neuen Ära

Zu Beginn des Informationszeitalters antizipieren Staaten gegenseitig ihre Aktionen und reagieren entsprechend; sie passen ihre Strategien an die Gegebenheiten an und entwickeln ihre Taktiken weiter, während sie dabei aktiv neue technologische und soziale Möglichkeiten nutzen. Erfolge werden kopiert und Misserfolge werden zu Erfahrungen. Derzeit deutet alles auf die Verbreitung und Weiterentwicklung von Tools sowie die Verfeinerung von Taktiken hin, die für Einflusskampagnen auf der ganzen Welt verwendet werden. Die Zahl jener Länder, die Desinformationskampagnen ausgesetzt waren, stieg zwischen 2017 und 2019 von 28 auf 70. Mindestens sieben Länder, darunter China, Indien, der Iran, Pakistan, Russland, Saudi-Arabien und Venezuela haben umfangreiche externe Einflusskampagnen über soziale Medien durchgeführt. Low-Tech-Tools zur Gestaltung und Verbreitung von Online-Nachrichten nehmen zu, und Dienste sind auf dem privaten Markt leicht und häufig offen verfügbar. Das bedeutet, dass in Informationen nun kampferprobte Taktiken verpackt sein können, die als Massenware zu haben sind.

Zukünftiger Informationskrieg

Darüber hinaus sind neu entstehende Fähigkeiten ein ernsthafter Grund zur Sorge. Rasche Fortschritte bei maschinellen Lernanwendungen ermöglichen erweiterte Fähigkeiten zur Realitätsverzerrung. Dazu gehört auch die Fälschung von bewegten Bildern, bekannt als Deepfakes. Weiters wird 5G einen Quantensprung bei der Anzahl der Informationsverbindungen und -sensoren in unseren Gesellschaften verursachen, die Übertragungsgeschwindigkeit von Informationen

drastisch erhöhen und die Einführung von Augmented-Reality- und Virtual-Reality-Applikationen in den 2020er-Jahren erleichtern. Dies wird die Art, wie Menschen Informationen aufnehmen, miteinander interagieren und die Realität erleben, stark beeinflussen.

Gegenstrategien für das Europa der Union

Die Folgen für die EU und ihre Mitgliedsstaaten sind tiefgreifend. Unverzerrte Diskurse sind eine Voraussetzung für das Funktionieren liberaler, demokratischer Gesellschaften. Wenn die digitalen Kanäle, die den freien Meinungsaustausch ermöglichen, manipuliert oder verstopft werden, so wird dies unsere demokratischen Diskurse beeinträchtigen und schrittweise unsere Demokratie beschädigen.

Jede wirksame Reaktion erfordert ein Paket defensiver und offensiver Maßnahmen. Es sollte sich auf drei Aspekte konzentrieren: die Erhöhung der Widerstandsfähigkeit unserer Gesellschaften, die Verstärkung der Schutzvorkehrungen gegen absichtliche Manipulation von Informationen in Netzwerken und schließlich die gemeinsame Ausrichtung einer Abschreckung.

Um die Resilienz unserer Gesellschaften zu erhöhen, brauchen wir mehr Investitionen in die Ausbildung auf Grund- und Mittelschulniveau sowie eine Neubelebung des Humboldt'schen Bildungsideals, das die Fähigkeit der Bürger, Informationen kritisch zu bewerten, sichern soll. Des Weiteren sollten zusammen mit dem Privatsektor verstärkt technologische Standards und Verfahren zur Bekämpfung der missbräuchlichen Verwendung von Social-Media-Plattformen geschaffen und kontinuierlich aktualisiert werden. Die politischen Entscheidungsträger müssen mehr technologische Kompetenz entwickeln, um geeignete Regulierungssysteme für Plattformanbieter schaffen zu können. Diese Systeme müssen drei miteinander konkurrierende Forderungen und Interessen in Balance halten: Sie sollten mit der liberal-demokratischen Struktur unserer Gesellschaften in Einklang gebracht werden und auf die Art und Schwere der Bedrohung durch Informationskriege eingestellt sein, ohne die Möglichkeiten für Innovation und Wirtschaftswachstum unnötig einzuschränken.

Schließlich sollten wir unseren Gegnern klarmachen, dass sie auf Informationskriege besser verzichten sollten, indem man internationale Normen schafft, die eine entsprechende Vorgehensweise auf der Grundlage eines klaren Verständnisses der gemeinsamen Interessen verbieten. Dazu bedarf es der Fähigkeit, alle offensiven Aktionen zu erwidern und den Gegner dort zu treffen, wo es weh tut, sodass auch in einer Grauzone Abschreckungsmaßnahmen gesetzt werden können. Derzeit sind die europäischen Kapazitäten in diesem Bereich unterentwickelt. Gleichzeitig gibt es nur wenig originelles und umsetzbares europäisches Denken in Bezug auf die Grundlagen einer hybriden Verteidigungshaltung. Die europäischen Staaten sollten ihre Bemühungen rasch auf die Entwicklung erforderlicher Abschreckungsfähigkeiten ausrichten und verstehen, wie diese synergistisch in einer Gesamtstrategie eingesetzt werden können. Alles in allem sind umsichtige Politiker gut beraten, sich schon heute auf die Informationskriege von morgen vorzubereiten.

Kernbotschaften

- Strategisch innovative Akteure haben in den letzten Jahren erfolgreich die Vernetzung moderner Gesellschaften ausgenutzt.
- Inzwischen haben die europäischen Regierungen eine Vielzahl von Gegenmaßnahmen ergriffen.
- Alle Indizien deuten auf die Verbreitung und Verbesserung von Instrumenten und die Verfeinerung der Taktiken für Informationskampagnen hin.
- Neue und neu entstehende Fähigkeiten sind ein ernsthafter Grund zur Sorge.
- Wirksame Gegenmaßnahmen gegen Informationskriegsführung sind die Bildung der Bevölkerung, bessere Schutzmaßnahmen durch Regulierung des Privatsektors und der Aufbau einer strategischen Abschreckung.

Autoreninformation

Dr. **Tim Sweijs**, geboren 1981, ist Forschungsdirektor am The Hague Centre for Strategic Studies (HCSS). Er ist Initiator, Ersteller und Autor zahlreicher Studien, Methoden und Tools für systemische Vorausschau, Frühwarnung, Konfliktanalyse, Bewertung des nationalen Sicherheitsrisikos sowie Strategie- und Kapazitätsaufbau. Sein Hauptforschungsinteresse gilt dem veränderten Charakter zeitgenössischer Konflikte. Er ist außerdem Senior Research Fellow an der Niederländischen Verteidigungsakademie, Mitglied des Zentrums für internationale Strategie, Technologie und Politik an der Sam-Nunn-Schule für internationale Angelegenheiten am Georgia Institute of Technology in den USA und dient als Berater für Technologie, Konflikt und nationales Interesse der Stabilisierungseinheit der britischen Regierung.