Forschung – Abschlussarbeiten

Die Achillesferse der Schweiz im Informationskrieg

Erkenntnisse aus dem Ukrainekrieg

KYRYLO PUSTOVIT

Abstract This article serves as a concise summary of a bachelor's thesis that evaluates information warfare in the Russian-Ukrainian conflict and its potential impact on Switzerland, particulary with regard to its security policy. The focus is placed on Russia's disinformation and propaganda tactics in the Ukraine war. Additionally, an analysis of Switzerland's security apparatus and cyber resilience has been undertaken to provide a holistic perspective. The empirical study, which was conducted by means of four interviews with experts from various relevant fields, resulted in four strategic options and five security policy recommendations. These include the development of a national strategy for information security, the promotion of international cooperation, raising societal awareness through a national campaign, the establishment of an analysis center for disinformation, and state subsidies in the area of cyber security for small and medium-sized enterprises. The aim of the paper is to raise awareness of disinformation in Swiss society and to provide a basis for further research. It could also contribute to the further development of security policy strategies.

Schlüsselbegriffe Desinformation; Propaganda; Informationskriegsführung; russisch-ukrainischer Konflikt; Sicherheitspolitik
Keywords information warfare; cyber warfare; disinformation; security policy; development options

KYRYLO PUSTOVIT wurde in Odessa (Ukraine) geboren und kam als Teenager in die Schweiz. Er erlangte seinen Bachelorabschluss in Business Communications an der Hochschule für Wirtschaft Zürich (HWZ) 2023, spricht sechs Sprachen fliessend und konnte umfassende berufliche Erfahrungen im OSINT-Bereich sammeln.
E-Mail: kyrylo.pustovit@outlook.com

Einleitung

Der russisch-ukrainische Konflikt hat seit der Krim-Annexion 2014 klar aufgezeigt, wie Informationskriegsführung pragmatisch und zielorientiert eingesetzt werden kann. Strategisch durchdachte und gut orchestrierte Desinformationskampagnen sind in der Lage, bestimmte Zielgruppen oder eine ganze Gesellschaft in einem Staat zu destabilisieren. Der geschickte Einsatz von Falschinformationen schafft in einer hochvernetzten Welt neue (Pseudo-)Realitäten. Die Grenzen zwischen Realität und Fiktion sind dementsprechend aufgrund der Opazität im Informationsraum schwer zu identifizieren, insbesondere dann, wenn die Falschinformationen systematisch verstreut werden. Ein wirksamer und präventiver Schutz gegen solche gezielten Angriffe erweist sich daher als komplex. Da eine solche Bedrohung auch hierzulande ernst zu nehmen ist, möchte ich in diesem Artikel die Auswirkungen des Ukrainekriegs auf die Sicherheitspolitik der Schweiz analysieren. Dabei wird der Fokus auf den Bereich Informationskriegsführung (Information Warfare) gesetzt, zumal die moderne Schweiz aufgrund ihrer globalen Vernetzung internationalen Informationsströmen stark ausgesetzt ist. Darüber hinaus bietet die Neutralität generell keine Immunität gegen Gefahren fremder Einmischung.

«Strategisch durchdachte und gut orchestrierte Desinformationskampagnen sind in der Lage, bestimmte Zielgruppen oder eine ganze Gesellschaft in einem Staat zu destabilisieren.»

«Darüber hinaus bietet die Neutralität generell keine Immunität gegen Gefahren fremder Einmischung.»

Es stellt sich also die Frage:

Welche sicherheitspolitischen Entwicklungsmöglichkeiten bieten sich für die Schweiz im Bereich Information Warfare aus dem russisch-ukrainischen Konflikt?

Wie funktioniert Information Warfare?

Die bedeutsamsten Werkzeuge von *Information Warefare* (IW) sind Desinformation und Propaganda. Beide Begriffe verweisen auf kommunikative Mittel, die zur Verfolgung eines bestimmten Ziels eingesetzt werden. Während *Propaganda* mit einseitiger und gezielter Kommunikation geführt wird, um bestimmte Ereignisse oder Meinungen hervorzuheben, verwendet sie nicht unbedingt Falschinformationen (Landesanstalt für Medien NRW, 2020). Es können gewisse Informationen verschwiegen oder ausgelassen werden, da im Fokus die Verbreitung eines bestimmten Narrativs steht. Die Informationen, welche diesem Narrativ keinen Nutzen erbringen, werden ausgeblendet.

Demgegenüber ist *Desinformation* die gezielte Verbreitung von Falschinformationen. Sie ist die taktische Auslegung der Kommunikation, die darauf abzielt, die schädlichen mit den nützlichen Informationen zu überlappen und somit den Empfänger zu täuschen und zu verwirren. Wenn Falschinformationen unabsichtlich und ohne das Wissen der veröffentlichenden Instanz, dass es sich um Falschinformationen handelt, weiterverbreitet werden, handelt es sich um Missinformation (Landesanstalt für Medien NRW, 2020). Die Tatsache, dass der letztgenannte Begriff in den Schweizer Medien kaum verwendet wird, zeugt von allgemeiner Unterschätzung der Gefahr und Problematik von IW hierzulande.

Das Wirkungspotenzial von Propaganda auf die Menschen in Bezug auf gewaltsame Konflikte wurde von David Yanagizawa-Drott, Professor an der Universität Zürich, untersucht. In einer Studie wurde die Rolle und der Einfluss eines Propaganda-Radiosenders auf die Zivilbevölkerung während des Völkermords in Ruanda im Jahr 1994 analysiert (Yanagizawa-Drott, 2014). Die Ergebnisse bestätigten, dass in den Dörfern mit besserem Signalempfang mehr Tötungen an der Tutsi-Minderheit stattfanden. Somit wurde bewiesen, dass die durch Massenmedien verbreitete Propaganda fähig ist, physische Gewalt innerhalb einer Gesellschaft im grossen Rahmen hervorzurufen. Elemente von Hasspropaganda im Einsatz von IW bergen deshalb ein enormes Bedrohungspotenzial.

Folglich bildet die gezielte *Medienmanipulation* ein weiteres Werkzeug der IW. Der Einsatz von manipulativen

Desinformationskampagnen kann politisch motiviert sein und auch von Regierungsbehörden sowie politischen Parteien durchgeführt werden. Um Verwirrung zu stiften, nutzen autokratische Regime die Medien und heutzutage oftmals auch soziale Netzwerke für die Verbreitung von Desinformation (Die Republik, 2020). Der ukrainische Journalist Peter Pomerantsev beschreibt diese Strategie als «Zensur durch Lärm»: Die Fake-News überfluten eine Gesellschaft so stark, dass man kaum mehr wahr von falsch unterscheiden kann (Kunz, 2020). Dieses ständige Rauschen fungiert in einer Gesellschaft somit als Ersatz für die Zensur, weil auf diese Weise der Fokus von der Wahrheit abgelenkt wird. Die Strategie und die Bekämpfung von IW sollte deshalb grundsätzlich im Interesse der nationalen Sicherheit eines jeden Staates liegen. Im Zeitalter der hybriden Bedrohungen, wo Kriege verschleiert und unangekündigt geführt werden, gilt es, die präventive Informationssicherheit zu schaffen, welche vor genau solchen Beeinflussungsversuchen schützt (BMVG, o.J.).

«Die Strategie und die Bekämpfung von IW sollte deshalb grundsätzlich im Interesse der nationalen Sicherheit eines jeden Staates liegen.»

Die Grenzen zwischen IW und CW (Cyber Warfare) sind oft fliessend, da die beiden Arten von Kriegsführung kombiniert eingesetzt werden können. Beispielsweise können durch einen Cyberangriff beschaffenen Informationen für eine anschliessende Desinformationskampagne verwendet werden. Hierbei ist auch die Informationssicherheit eng mit der Cybersicherheit verknüpft, da der Cyberraum als wichtigste Plattform für die Verbreitung von Information in der heutigen, global vernetzten Welt fungiert.

Die Schweizer Konzeption und Organisation

Ein Ziel meiner Bachelorarbeit war es, die Veränderungen im Schweizerischen Sicherheitsappart als Folge des Ukrainekriegs zu beobachten. Es gilt deshalb, zunächst eine Gesamtübersicht der für die Fragestellung relevanten Schweizer Cyber- und Informationssicherheits-Infrastruktur vor dem russischen Grossangriff im Februar 2022 zu erstellen.

Sicherheitsorgane

In der Schweiz ist die Organisation der Cyber- und Informationssicherheit nicht vollumfänglich zentralisiert, sondern auf mehrere Stellen verteilt. Auf Bundesebene ist das VBS für die Cyberabwehr im Rahmen der Landesverteidigung und der Nationalen Strategie für Cybersicherheit (NCS) zuständig. Innerhalb des VBS sind diverse Schnittstellen bei der Erfüllung dieser Aufgabe im Cyberraum aktiv:

- Der Nachrichtendienst des Bundes (NDB) ist für die sicherheitspolitische Bekämpfung der von einem Fremdstaat ausgeführten Cyberangriffe zuständig (VBS, 2022a). Der NDB spielt für die Schweizer Regierung eine essenzielle Rolle in der sicherheitspolitischen Einschätzung. Jährlich wird vom NDB ein Bericht erstellt, in welchem die wichtigsten Lageentwicklungen aus nachrichtendienstlicher Sicht identifiziert, ausgewertet und – soweit strategisch zielführend – der Öffentlichkeit vorgestellt werden.
- Der Nachrichtendienst der Armee (NDA) umfasst alle Armeetruppen, die nachrichtendienstliche Aufgaben erfüllen. Der Militärische Nachrichtendienst der Armee (MND) innerhalb des NDA ist unter anderem damit beauftragt, für die Armee signifikante Informationen aus dem Ausland zu beschaffen und die Entwicklung ausländischer Streitkräfte zu verfolgen (Schweizer Armee, o.J.a).
- Der Schwerpunkt in der Gesamtkonzeption Cyber liegt auf der zukünftigen Cyberausrichtung der Schweizer Armee. Das Kommando Cyber, welches als Nachfolger und damit auch als Weiterentwicklung der Führungsunterstützungsbasis (FUB) ist, wurde per 1. Januar 2024 operationell (VBS, o.J.).
- Der im Jahr 2019 gegründete Cyber-Defence Campus (CYD) dient als Schnittstelle zwischen VBS, Wirtschaft und Wissenschaft im Bereich Cyberabwehr (armasuisse, 2022). Der CYD, welcher teilweise aus Experten von armasuisse besteht, evaluiert neue Abwehransätze, setzt sich mit den neuen Technologie-Trends auseinander und sucht gleichzeitig auch nach Schwachstellen in den bestehenden Systemen.

NCSC und Kantone

Eine zentrale Rolle im Bereich der Organisation der Cyberabwehr in der Schweiz spielt

das Nationale Zentrum für Cybersicherheit (NCSC). Es gilt als erste Anlaufstelle auf nationaler Ebene für die Bevölkerung, Wirtschaft und Verwaltung und koordiniert die Cybersicherheit mithilfe von zahlreichen Schnittstellen in der Schweiz (NCSC, 2022a). Obschon die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) dem VBS als Strategiegrundlage dient und dezentral umgesetzt werden soll, erfordert sie ebenso Aufsichts- und Koordinationsaufwand seitens NCSC. Das NCSC ist in diesem Zusammenhang zugleich für den Cyberschutz von Objekten kritischer Infrastruktur verantwortlich. Diesbezüglich ist die vom NCSC geführte Melde- und Analysestelle Informationssicherung (MELANI) zu erwähnen. MELANI bildet den Kern des NCSC und unterstützt die Betreiber der kritischen Infrastruktur mit technischen und nachrichtendienstlichen Analysen bei potenziellen Cyberangriffen.

Trotz des föderalistischen Systems in der Schweiz erfordert eine nachhaltige Cybersicherheitsorganisation einen möglichst einheitlichen Aufbau oder zumindest eine kooperative Organisationsstruktur, die Herausforderungen effizient angehen kann. Da jeder Kanton ein bestimmtes Mass an Autonomie in der Gestaltung der eigenen Sicherheitspolitik geniesst, unterscheidet sich die Organisation der Cybersicherheit auf kantonaler Ebene beträchtlich. Einige Kantone verfügen über eigene kantonale Cybersicherheitsbehörden oder haben ihre Kantonspolizei oder ihr kantonales Amt für Informatik und Telekommunikation damit beauftragt. Es gibt dennoch gemeinsame Merkmale der kantonalen Cybersicherheitsstrategien. Nebst der Kooperation mit den Bundesbehörden arbeitet das NCSC ebenfalls eng mit den Kantonen zusammen und unterstützt so beispielsweise alle kantonalen Polizeibehörden bei der Verfolgung und Aufklärung von Straftaten im Zusammenhang mit Cyberkriminalität. Da es sich auch oftmals um interkantonale oder sogar internationale Fälle handelt, ist unterdies die enge Zusammenarbeit zwischen der Bundesanwaltschaft (BA) und dem Bundesamt für Polizei (fedpol) zwangsläufig (SVS, 2021).

Die Schweizer Strategie

Obschon der Bundesrat eine aktive Rolle bei der Koordinierung des Schutzes und der Reaktion auf Vorfälle übernehmen muss, liegt der Schutz vor Cyberrisiken in der geteilten Verantwortung zwischen Staat, Gesellschaft und Wirtschaft. Diese müssen sich grundsätzlich um ihren eigenen Schutz kümmern, während das NCSC sie dabei mit Kooperation und bewährten Verfahren unterstützt (NCSC, 2018). Zu diesem Schluss kam das NCSC bereits im Jahr 2018. Die damalige Lagebeurteilung trug den Namen «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022» und bot eine nationalstrategische Basis bis Jahr 2022 für die Präventionsverbesserung, Früherkennung, Reaktion und Widerstandsfähigkeit in allen Bereichen, die mit Cyberrisiken zusammenhängen (NCSC, 2018).

An dieser Stelle möchte ich eine kritische Anmerkung anbringen. Keine der sieben strategischen Ziele der NCS 2018-2022 erwähnen explizit eine systematische Früherkennung oder Bekämpfung von Desinformationskampagnen oder ausländischen Propaganda-Elementen im Schweizer Cyberraum. Alle Bedrohungstypen im Cyberbereich, darunter auch Desinformation und Propaganda, werden subsumierend als Cyberrisiken oder Cybervorfälle aufgeführt. Bei den strategischen Zielen unterscheidet man demnach nicht zwischen einem Cyberangriff auf ein regionales Elektrizitätswerk oder einer massiven Desinformationskampagne, die den Ausgang einer nationalen Volksabstimmung beeinflussen kann.

«Keine der sieben strategischen Ziele der NCS 2018-2022 erwähnen explizit eine systematische Früherkennung oder Bekämpfung von Desinformationskampagnen oder ausländischen Propaganda-Elementen im Schweizer Cyberraum.»

Dieser Ansatz muss verbessert werden: Die Bedrohungslage sollte nach Eintrittswahrscheinlichkeit und Schadensausmass ins Verhältnis gesetzt oder zumindest die Bedrohungstypen müssten nach Priorität der Behandlung skaliert werden. Eine integrierte Risikoanalyse würde die strategischen Ziele gegeneinander abwägen. Denn alleine das Verständnis, dass man die Desinformation und Propaganda nicht als ein weiteres Cyberrisiko verallgemeinern sollte, könnte die notwendige Ernsthaftigkeit bei der Problembekämpfung innerhalb einer Gesellschaft begünstigen.

Die Rede sollte deshalb nicht mehr von generellen Cyberrisiken sein, sondern es muss eine konkrete Bedeutung und Relevanz bereits in der Terminologie erkennbar sein. Zum Vorbild kann man sich dazu die nationale Cybersicherheitsstrategie Frankreichs nehmen, die ausdrücklich den Begriff «digitale Sicherheit» (fr. la sécurité du numérique) anstelle «Cybersicherheit» verwendet (ANSSI, o.J.).

Die Schweizer Fähigkeit

Die Schweiz ist aufgrund ihrer Rolle als internationaler Standort (insbesondere die Region Genf) für zahlreiche Organisationen, Konzerne und Technologien ein attraktives Ziel für Spionageaktivitäten ausländischer Nachrichtendienste (NDB, 2020). Diese Aktivitäten können sowohl politische Institutionen und kritische Infrastrukturen als auch internationale Unternehmen und Organisationen betreffen und gefährden somit die Schweizer Interessen und Sicherheit. Der Nachrichtendienst des Bundes (NDB) konzentriert sich dabei auf die aktivsten ausländischen Nachrichtendienste, die aggressiv gegen die Schweizer Interessen vorgehen. In den letzten Jahren wurden von Nachrichtendiensten verstärkt Cyberangriffe in der Schweiz verzeichnet, vorwiegend durch Staaten wie Russland, Nordkorea, China und Iran, die auch internationale Organisationen und Forschungseinrichtungen ins Visier genommen haben (NDB, 2020). Die grösste Bedrohung für die Schweiz stellen daher die russischen, chinesischen, türkischen und iranischen Nachrichtendienste dar (NDB, 2020). Die beiden letzten operieren jedoch mit eher bescheidenen Mitteln in der Schweiz. Die chinesischen Nachrichtendienste setzen in der Schweiz oftmals auch Offiziere unter nichtoffizieller Tarnung ein, welche beispielsweise als Touristen, Studenten, Forscher oder Geschäftsleute auftreten.

Doch hauptsächlich für die russischen Nachrichtendienste gilt die Schweiz als ein wichtiger europäischer Umschlagplatz, weshalb sie auch auf Schweizer Boden besonders aktiv sind. Tatsächlich wird hierzulande bis zu einem Drittel des offiziell akkreditierten Vertretungspersonals als mögliche Angehörige eines russischen Geheimdienstes identifiziert oder verdächtigt (NDB, 2019). Auch in anderen europäischen Ländern ist die Präsenz russischer Geheimdienste in den letzten Jahren spürbar geworden.

Die russische IW

Der russisch-ukrainische Konflikt zeichnet sich durch eine tiefverwurzelte Auseinandersetzung aus, bei welcher Desinformation und Propaganda insbesondere seitens des Aggressors vermehrt zum Einsatz kommen. Eine essenzielle Rolle spielen dabei die russische Sprache und die russisch-orthodoxe Kirche im Gesamtkontext der «russischen Welt». Die primäre Rechtfertigung für die russische Aggression gegenüber der Ukraine seit 2014 ist der vermeintliche Schutz der russischsprachigen Bevölkerung vor ukrainischen Neonazis. Die russische Propaganda verwendet ausgefeilte Narrative samt Falschinformationen aus historischen sowie aktuellen Ereignissen und ist stets flexibel. Sie greift die Schwächen der westlichen Demokratie frontal an. Eine offensichtliche Intention ist es, durch die Verbreitung mehrerer möglichen Versionen über bestimmte Ereignisse Zwietracht zu säen und Misstrauen gegenüber der offiziellen Berichterstattung sowie der staatlichen Institutionen im jeweiligen Staat des Empfängers zu wecken. Die Desinformationskampagnen zum Flug MH17 und zum Giftanschlag in Salisbury sind dabei Musterbeispiele auf internationaler Ebene. Es soll eine Widersprüchlichkeit der offensichtlichen Ereignisse entstehen, um Zielpersonen mit der Vielfalt möglicher plausibler Erklärungen zu überfordern und sie so von der Wahrheit fernzuhalten. Das Zielpublikum soll durch die eigene Verunsicherung zum Schluss kommen, dass nicht alles so eindeutig und klar sei.

Die böswillige Absicht und ihre Wirkung bleiben aber auch in den westlichen demokratischen Gesellschaften meist unerkannt, da dort ein Mass an kritischem Hinterfragen Teil der öffentlichen Meinungsbildung ist. Permanente Diffamierung durch diskreditierende Berichterstattung beeinflusst diese Meinungsbildung jedoch in eklatanter Weise. Zusätzlich wird die Informationsquelle beim online-Medienkonsum selten recherchiert, was eine grundsätzliche Verwundbarkeit gegenüber Fake-News darstellt. Es werden Meinungen vermeintlicher Experten herangezogen und Quellen aus durch den Kreml finanzierte Publikationsstellen zitiert. Dadurch entsteht das falsche Bild, dass die russische Interpretation des Weltgeschehens weltweit verbreitet ist und dass es im Grunde sinnlos ist, Russland auf der Weltbühne zu isolieren.

Die sicherheitspolitische Reaktion der Schweiz

Nach der Eskalation des Konflikts am 24. Februar 2022 sahen mehrere politische Parteien die Revision der Verteidigungspolitik und Modernisierungsbedarf der Schweizer Armee als notwendige Schritte.

Diesbezüglich erklärte der Bundesrat in der Stellungnahme auf die Interpellation 22.3363 im März 2022 den Ausbau der Cyberfähigkeiten sowie Luftraumverteidigung als oberste Priorität (Das Schweizer Parlament, 2022a). Die Modernisierung in den anderen Bereichen der Armee, wie beispielsweise neue Systeme der Bodentruppen, Aufklärung und Führungsunterstützung, musste deshalb zeitlich nach hinten verschoben werden. Der Bundesrat erwähnte auch die steigenden Kosten der IT-Systeme, weshalb eine Erhöhung der Armeeausgaben notwendig sei. Die entsprechenden Motionen wurden im Juni 2022 angenommen (Das Schweizer Parlament, 2022b). Für die Kosten der Armee wird somit ein Ausgabenziel von mindestens 1% des BIP bis 2030 festgelegt (Das Schweizer Parlament, 2022c).

Vor allem finanzpolitische Überlegungen haben aber nun dazu geführt, dass sich das Parlament im Dezember 2023 jedoch dafür entschieden hat, das 1% Ziel auf 2035 zu verschieben. Im Frühling 2024 wird der Bundesrat dem Parlament mit der Armeebotschaft 2024 die Ausrichtung der Armee bis 2035, den Zahlungsrahmen von 2025-2028 und Verpflichtungskredite für konkrete Beschaffungen vorstellen (VBS, 2023).

Parallel zum politischen Diskurs über die Armeemodernisierung wurde 2022 auch die Frage zum NATO-Verhältnis im Ständerat debattiert. Die Debatte über die NATO-Mitgliedschaft neutraler europäischer Staaten wurde unmittelbar nach dem russischen Einmarsch wiederaufgenommen. Anders als Schweden und Finnland wird für die Schweiz jedoch keine NATO-Mitgliedschaft in Aussicht gestellt. Ein wichtiger Grund dafür ist die Schweizer Neutralität (Swissinfo, 2022). Darüber hinaus ist der Rückhalt in der Schweizer Bevölkerung laut einer aktuellen Umfrage für einen NATO-Beitritt gering (Der Bundesrat, 2023a). Dennoch: Eine mögliche Annäherung an die NATO wird seit Januar 2023 von einer knappen Mehrheit (55%) der Schweizer befürwortet. Eine NATO-Annäherung findet bereits in Form gemeinsamer Militärübungen statt. In 2022 und 2023 beteiligte sich die Schweizer Armee an der internationalen Cyberübung «Locked Shields». Dabei wird der Schutz kritischer Infrastruktur vor Cyberangriffen in einem hybriden Bedrohungsszenario trainiert (Netzwoche, 2022).

Die Rolle, Bedeutung und mögliche Anpassung der Schweizer Neutralität wurden im In- und Ausland diskutiert. Insbesondere nach der verweigerten Weitergabe von Waffen in die Ukraine im März 2023 wurde an der Schweiz heftige Kritik aus dem Ausland geübt. US-Botschafter Scott Miller fand dafür in einem NZZ-Interview ebenfalls klare Worte und bezeichnete das Verhalten der Schweiz im Zusammenhang mit dem Wiederausfuhrverbot als «nicht neutral» (NZZ, 2023, o. S.). Millers deutlicher Kritikpunkt war auch die Einfrierung von nur 7,75 Milliarden Franken durch Schweizer Banken, einem Bruchteil der geschätzten Vermögenswerte russischer Oligarchen hierzulande. In diesem Kontext forderte Miller die Schweiz dringend auf, an der Task-Force «Russian Elites, Proxies and Oligarchs» (REPO) teilzunehmen.

Die Überführung des NCSC vom EFD zum VBS ist eine ebenso relevante Umstrukturierung in diesem Kontext. So wurde im Dezember 2022 beschlossen, das NCSC als neues Bundesamt für Cybersicherheit (BACS) und als Organisationseinheit des VBS per 1. Januar 2024 zu lancieren. Die Vernetzung des NCSC in den Staatsstrukturen sowie in Gesellschaft und Wirtschaft sollen zusammen mit den Technologien und Fähigkeiten des VBS die Resilienz in der Cyberabwehr erhöhen (VBS, 2022c). Laut der zuständigen Bundesrätin und Departementschefin des VBS, Viola Amherd, soll das neue Bundesamt speziell die zivile Cybersicherheit stärken. Das neue Bundesamt für Cybersicherheit wird auch eigene Supportaufgaben wie Finanzen, Personal, Informatik und Recht selbstständig übernehmen. Daher wird das Budget zur Schaffung von vier zusätzlichen Stellen um 0,8 Millionen Franken erhöht (Der Bundesrat, 2023b). Das bereits vom EFD eingeplante Budget von 13,7 Millionen Franken wird ohnehin ins neue Bundesamt übertragen.

In diesem Kontext steht ebenfalls die Schaffung des neuen Staatssekretariats für Sicherheit (SEPOS) im VBS. Angesichts der zunehmenden hybriden Bedrohung und der Anspannung der aktuellen geopolitischen Lage wurde damit auch eine Behörde geschaffen, die die sicherheitspolitische Koordination übernimmt und den zivilen Sicherheitsbereich stärkt (VBS, 2023). Das

neue Kompetenzzentrum für Sicherheitspolitik ist seit dem 1. Januar 2024 aktiv und untersteht mit seinen rund 100 Mitarbeitenden direkt Bundesrätin Viola Amherd. Am 22. Dezember 2023 wurde Dr. Markus Mäder zum Staatssekretär für Sicherheitspolitik im VBS vom Bundesrat ernannt. Zusätzlich wurde bekanntgegeben, dass Bundesrätin Amherd Pälvi Pulli ab dem 1. Januar 2024 zur stellvertretenden Staatssekretärin ernannt hat, wofür ihr der Bundesrat den Botschaftertitel verliehen hat (VBS, 2023). Pälvi Pulli, die als sicherheitspolitische Expertin auch ausserhalb der Landesgrenzen gilt, wird die Bereiche Strategie und Kooperation im SEPOS leiten.

Empirische Untersuchung

Ein weiteres Ziel der Bachelorarbeit war es, neben den vorhandenen Erkenntnissen aus der Theorie, welche ein Basisverständnis der gesamten Thematik bilden, zusätzliche Informationen zur Beantwortung der gestellten Forschungsfrage zu gewinnen. Für die empirische Untersuchung der gestellten Forschungsfrage wurde die qualitative Datenerhebung gewählt, da sich die quantitative Forschung als ungeeignet in der vorhandenen Fragestellung erweist.

Dazu wurden mittels Experteninterviews die bisherigen Erkenntnisse durch Expertenmeinungen ergänzt. Die subjektiven Meinungen, Ansichten und Erfahrungen der Experten spielen dabei eine zentrale Rolle. Die Fachkenntnisse dieser Experten sollen das Gesamtbild vervollständigen, was zur Beantwortung der Forschungsfrage notwendig ist. Es wurden fachkundige Experten aus den Bereichen Sicherheitspolitik, Technologie, Cyber- und Informationssicherheit sowie Militär zu einem Experteninterview eingeladen. Ihr Fachwissen aus den für die IW relevanten Bereichen war in der Lage, die thematischen Lücken zu schliessen, damit eine interdisziplinäre Lösung vorgeschlagen werden kann.

SWOT-Analyse

Nach dem die Daten aus den Experteninterviews anhand von zuvor gebildeten Kategorien «Staat», «Privatwirtschaft», «Zivilgesellschaft» und «Ausland» ausgewertet wurden, konnten eine SWOT-Analyse sowie einige strategischen Empfehlungen ausgearbeitet werden. Im Zentrum der SWOT-Analyse stand die Aufstellung im Bereich der IW der Schweiz als Staat sowohl auch als Gesellschaft.

In einem ersten Schritt wurden die Stärken, Schwächen, Chancen und Risiken wie folgt definiert:

Zu den *Stärken* zählen die Durchlässigkeit zwischen der Bildungslandschaft und staatlichen Behörden sowie das Milizprinzip, welches die Bürgerbeteiligung an der Sicherheit stärkt. Eine weitere Stärke ist zweifellos die florierende Cybersicherheitsbranche, die das Abwehrfundament gegen digitale Bedrohungen bildet und zum Schutz der IT-Infrastruktur massiv beiträgt. Dafür ist auch die Bereitstellung von finanziellen, technologischen und personellen Ressourcen unerlässlich. Eine mündige Gesellschaft und Schwarmintelligenz sind weitere und nicht weniger signifikante Stärken der Schweiz im IW-Bereich.

Selbstverständlich konnten auch einige *Schwächen* aus der Datenanalyse festgestellt werden. Ein zentrales Defizit stellt das fehlende Bewusstsein sowie das Verständnis der Schweizer Gesellschaft in der Informations- sowie Cybersicherheit dar. Die Unentschlossenheit bei politischen Entscheiden, bedingt durch die schweizerische Konkordanzpolitik, manifestiert sich als politische Trägheit in Bezug auf wichtige Entscheide im IW-Bereich. Zudem herrscht innerhalb der Schlüsselbehörden ein sogenanntes Silodenken, welches zu fehlender Strategiebündelung und zu einer mangelnden Koordination dieser führt. Letztlich besteht auf internationaler Ebene eine markante Diskrepanz zwischen dem hochentwickelten Innovationsklima und der hinterherhinkender staatlichen Cybersicherheit, die sich im niedrigen Ranking der Schweiz in internationalen Cybersicherheits-Indices zeigt.

«Ein zentrales Defizit stellt das fehlende Bewusstsein sowie das Verständnis der Schweizer Gesellschaft in der Informations- sowie Cybersicherheit dar.»

Als nächstes werden die Chancen innerhalb der SWOT-Analyse präsentiert. Die Sensibilisierung und Aufklärung der Schweizer Bevölkerung hinsichtlich dieser

eher komplexen Thematik bietet sich als eine wesentliche Chance. Der Erfahrungsaustausch mit internationalen Organisationen und Behörden sowie der Ausbau der internationalen Kooperation im neu geschaffenen Staatssekretariat für Sicherheit stellen eine weitere zentrale Chance zur Stärkung der Schweiz dar. In Bezug auf das neu strukturierte Bundesamt für Cybersicherheit ist die Involvierung der Privatwirtschaft und der Zivilgesellschaft ebenso prospektiv.

«Eine Überbewertung von finanzpolitischen Fragen kann zur Verdrängung und zur Vernachlässigung der sicherheitsrelevanten Interessen führen.»

Zuletzt müssen die *Risiken* definiert werden. Die allgemeine Unterschätzung der Bedrohung durch Desinformation und der Akteure kann zu einer gesteigerten Anfälligkeit für Beeinflussungsoperationen in der Gesellschaft sowie im Staat als Ganzes führen. Eine Überbewertung von finanzpolitischen Fragen kann zur Verdrängung und zur Vernachlässigung der sicherheitsrelevanten Interessen führen. Daraus könnte sich ein fehlgeleitetes Beurteilungsvermögen entwickeln, welches zu negativen politischen Entscheidungen führen kann. Eine negative Wahrnehmung der Schweiz vom Ausland à la «Trittbrettfahrerin der europäischen Sicherheit» ist ein weiteres bedeutsames Risiko. Schliesslich birgt eine misslungene politische Trenderkennung, wo aufkommende Bedrohungen nicht rechtzeitig erkannt und adressiert werden, die grösste Gefahr.

In einem zweiten Schritt gilt es, die Ergebnisse im Hinblick auf mögliche strategische Empfehlungen auszuwerten. Dies kann mittels Kombinierung sowie gegenseitiger Gegenüberstellung der einzelnen Kategorien erfolgen.

S-O-Strategie
Sind die Stärken vorhanden, damit die Chancen genutzt werden können?

W-O-Strategie
Werden die Chancen aufgrund der Schwächen verpasst?

S-T-Strategie
Mit welchen Stärken werden die Risiken begegnet?

W-T-Strategie
Welchen Risiken ist man aufgrund der Schwächen ausgesetzt?

In einem dritten und letzten Schritt entstehen mögliche strategische Optionen für die Schweiz, die anhand von Erkenntnissen aus der Datenauswertung und der SWOT-Analyse näher beschrieben werden.

S-O-Strategie

Die genannten Stärken reichen vollständig aus, um die möglichen Chancen zu nutzen. Insbesondere im Ressourcenbereich hat die Schweiz einzigartige Vorteile beispielsweise gegenüber anderen europäischen Ländern, die mit einer möglichen Ressourcenknappheit zu kämpfen haben. Dies geht über den finanziellen Bereich hinaus, zumal die Schweiz ebenso viel technologisches Know-how besitzt. Auch die Forschung geniesst einen hohen Stellenwert hierzulande. Die Schweizer Gesellschaft hat ein hohes Mass an kollektiver Intelligenz und kann daher auf die Problematik der IW sensibilisiert werden. Die Cybersicherheitsbranche kann ebenso ungehindert in die Zusammenarbeit mit den staatlichen Behörden und speziell in das neue Bundesamt für Cybersicherheit einbezogen werden. Die internationale Kooperation des neuen Staatssekretariats für Sicherheit ist auch aufgrund starker Vernetzung der Schweiz auf internationaler Ebene realisierbar.

S-T-Strategie

Innerhalb dieser strategischen Option gibt es einige Herausforderungen, die einen politischen Willen voraussetzen, zumal allein die Ressourcen dafür nicht ausreichen. Dies gilt insbesondere für die Überbewertung der finanzpolitischen Entscheide, die möglicherweise die sicherheitspolitischen Interessen vernachlässigen oder ignorieren können. Eine mögliche Strategie diesbezüglich ist die Beratung durch die Forschung sowie zahlreiche Institute, welche die notwendigen und umfassenden Lage- und Umfeldanalysen für politische Entscheide liefern können. Damit könn-

ten auch mögliche Fehler bei der Erkennung der politischen Trends vermieden werden. Zudem kann die Stärke der Schweizer Cybersicherheitsbranche für eine aktive Zusammenarbeit mit internationalen Behörden genutzt werden, sodass auch die Wahrnehmung im Ausland positiv beeinflusst wird.

W-O-Strategie

Hier können gleichzeitig mehrere Chancen verpasst werden, da die ausgewerteten Schwächen sich mehrmals mit den Chancen direkt überschneiden. Ein fehlendes Bewusstsein kann Grund dafür sein, dass der Einbezug der Zivilgesellschaft und Privatwirtschaft in das neue Bundesamt für Cybersicherheit sowie andere Behörden nicht wahrgenommen wird. Mit dem fehlenden Bewusstsein der Gesellschaft können auch die Aufklärungsversuche der Bevölkerung verpasst werden. Die politische Unentschlossenheit und Trägheit können den Erfahrungsaustausch mit internationalen Behörden und Organisationen hinauszögern oder komplett verhindern. Ebenso kann eine fehlende Strategie dazu führen, dass das neue Staatssekretariat für Sicherheit (SEPOS) eine weitere Beratungsfunktion übernimmt und keine proaktive Haltung einnehmen kann.

«Ebenso kann eine fehlende Strategie dazu führen, dass das neue Staatssekretariat für Sicherheit (SEPOS) eine weitere Beratungsfunktion übernimmt und keine proaktive Haltung einnehmen kann.»

W-T-Strategie

Die grössten Gefahren und Risiken für die Schweiz bergen sich in dieser strategischen Option und sind somit auch prioritär zu behandeln. Es besteht ein Risiko, dass die Schweiz anfällig für mögliche Beeinflussung durch Desinformation sein könnte. Durch das fehlende Bewusstsein kann auch die damit verbundene Gefahr aufgrund vom täuschenden Sicherheitsgefühl nicht frühzeitig erkannt werden. Oder die Beeinflussungsversuche werden erst dann erkannt, wenn es bereits zu spät ist und die öffentliche Meinung dadurch bereits beeinflusst wurde. Das Risiko, dass sich solche Operationen auch in den wichtigen politischen Entscheiden wie Volksabstimmungen abfärben können, sollte ernst genommen werden. Zusätzlich besteht durch die politische Unentschlossenheit und die fehlende Strategie auch das Risiko, dass die negative Wahrnehmung der Schweiz sich weiter verschlechtert. Das Narrativ der «Trittbrettfahrerin der europäischen Sicherheit» würde sich somit auf internationaler Ebene weiter ausdehnen. Dies könnte auch die Schweizer Exportwirtschaft, einschliesslich der Rüstungsindustrie, beeinträchtigen.

Fazit

Die durchgeführte qualitative Untersuchung verdeutlicht, dass in der Schweizer Gesellschaft ein Mangel an Bewusstsein für die Risiken und Auswirkungen der Desinformation besteht. Die fehlende einheitliche Strategie der relevanten Sicherheitsbehörden belegt ebenfalls eine Unterschätzung dieser Problematik auf Staatsebene, was grundsätzlich die Gefahr der Beeinflussbarkeit durch IW erhöhen kann. Trotzdem kann die Schweiz zahlreiche Stärken aufweisen, mit welchen sie die vorhandenen Schwächen überwinden kann. Nebst erforderlichen finanziellen sowie technologischen Ressourcen besitzt die Schweiz auch ein hohes Mass an Schwarmintelligenz, die sich vermutlich mit dem hohen Bildungsstand hierzulande verbinden lässt. Somit kann auch ein proaktiver und lösungsorientierter Ansatz entstehen, der mögliche Gefahren im Bereich IW umgehen kann. Aus den vorliegenden Erkenntnissen lassen sich nun folgende Weiterentwicklungsmöglichkeiten in Form von praxisbezogenen Empfehlungen für die Schweiz definieren. Die einzelnen Bereiche für Verbesserungsmassnahmen wurden analog zu den vorhin gebildeten Kategorien strukturiert. Somit wurden zwei Empfehlungen für die Kategorie «Staat», ebenso viel für die Kategorie «Zivilgesellschaft» und eine für die Kategorie «Privatwirtschaft» entwickelt.

Staat

- Die Entwicklung einer nationalen Strategie im Kampf gegen Beeinflussungs- und Informationsoperationen, Desinformationskampagnen und fremdstaatliche Propaganda soll die Schwächen der Schweiz im Bereich IW mindern. Diese Strategie soll eine koordinierende Funktion in der Zusammenarbeit zwischen den relevanten Bundesbehörden und -stellen erfüllen. Des Weiteren sollte sich diese

Strategie auch mit der Struktur von Konkordaten befassen, damit die Zusammenarbeit und Organisation zwischen Kantonen gefördert werden können. Im Vergleich zur NCS 2018-2022 soll sie auch semantisch umfassender gestaltet werden, und den Begriff «Cyber» mit «digitaler Sicherheit», «digitaler Souveränität» oder «ziviler Informationssicherheit» ersetzen. Auch zwecks einer positiven internationalen Wahrnehmung ist es zentral, dass die bedeutenden Elemente der aussenpolitischen Strategie in die Erarbeitung der neuen Strategie für digitale Sicherheit eingebunden werden.

«Die Entwicklung einer nationalen Strategie im Kampf gegen Beeinflussungs- und Informationsoperationen, Desinformationskampagnen und fremdstaatliche Propaganda soll die Schwächen der Schweiz im Bereich IW mindern.»

- Die Förderung der internationalen Zusammenarbeit der Schlüsselbehörden würde die Wirksamkeit und Fähigkeiten der Schweizer Sicherheitsorgane im Bereich Informations- und Cybersicherheit deutlich erhöhen. Mit der Schaffung des neuen Staatssekretariats für Sicherheit (SEPOS) innerhalb des VBS bieten sich nun zahlreiche Optionen in der Gestaltung der Zusammenarbeit auf internationaler Ebene. So könnte es beispielsweise mit dem Zentrum für strategische Kommunikation des ukrainischen Ministeriums für Kultur und Informationspolitik eine Kooperation eingehen. Eine weitere enge Kooperation mit der East StratCom Task Force vom Europäischen Auswärtigen Dienst wäre ebenfalls lehrreich, da diese bereits seit 2015 den russischen Desinformationskampagnen entgegenwirkt. Nebst der Armee kann auch das neue Bundesamt für Cybersicherheit mit den Partnerbehörden der NATO-Staaten zusammenarbeiten und dadurch auch die notwendigen Erfahrungen im Bereich IW sammeln. Der Fokus soll hierbei auf den Austausch von Informationen und bewährten Verfahren gelegt werden.

Zivilgesellschaft

- Die Sensibilisierung und Förderung des Bewusstseins der Gesellschaft ist eine essenzielle Massnahme, die im zivilgesellschaftlichen Bereich unternommen werden soll. Dies kann in Form einer nationalen Awareness-Kampagne erfolgen und zur Erreichung möglichst vieler Zielgruppen auf mehreren Kanälen durchgeführt werden. Speziell für die jüngere und Social-Media-affine Bevölkerungsgruppe kann die Kampagne online sowie direkt an Bildungseinrichtungen durchgeführt werden. Das Ziel dieser Awareness-Kampagne sollte es sein, das Bewusstsein der Zivilgesellschaft für die Bedrohung der Fake-News, Desinformation und Missinformation zu schärfen. Dabei müssen die Informationssicherheit und digitale Sicherheit der gesamten Gesellschaft in den Vordergrund gestellt werden. Bekanntermassen fühlt sich die breite Öffentlichkeit nicht angesprochen, wenn hauptsächlich von Cybersicherheit die Rede ist. Denn die bewusste Einrichtung eines sicheren Passwortes durch die Bevölkerung allein ist nicht in der Lage, eine umfassende Informations- und Cybersicherheit zu gewährleisten. Ebenso muss die Gefahr der Beeinflussbarkeit im Netz klar kommuniziert werden, damit ein gesundes Mass an kritischem Denken auf gesellschaftlicher Ebene entstehen kann. Die Gesellschaft sollte daher angeregt werden, die Quelle eigenständig zu überprüfen oder zumindest zu hinterfragen. Auf diese Weise kann das Immunsystem einer Gesellschaft im Kampf gegen Desinformationskampagnen gestärkt werden. Auch angesichts der künftigen Entwicklung von KI-generierter Desinformation in visueller Form hat eine solche Awareness Kampagne eine hohe Relevanz für die Schweizer Gesellschaft.

«Die Sensibilisierung und Förderung des Bewusstseins der Gesellschaft ist eine essenzielle Massnahme, die im zivilgesellschaftlichen Bereich unternommen werden soll. Dies kann in Form einer nationalen Awareness-Kampagne erfolgen und zur Erreichung möglichst vieler Zielgruppen auf mehreren Kanälen durchgeführt werden.»

- Die Einrichtung des Analysezentrums für Desinformation in der Schweiz wäre eine weitere Empfehlung im zivilgesellschaftlichen Bereich. Analog zu «EU vs. Disinfo» würde dieses Analysezentrum als eine schweizweite Plattform zur Aufklärung der Bevölkerung dienen. Da sich einige Experten gegen staatliche Eingriffe im Umgang mit Medien ausgesprochen haben, kann das Analysezentrum für Desinformation auch eine Nicht-Regierungs-Organisation, NGO (Non-Governmental Organization) sein. Gleichzeitig muss sie aber eine NPO (Non-Profit Organization) sein, zumal hinter der Entlarvung von Desinformation kein wirtschaftliches Interesse versteckt sein darf. Dieses Zentrum würde regelmässig die Berichterstattung aller bedeutenden online- und Print-Medien der Schweiz prüfen, mit dem Ziel, Fact-Checking und Desinformationserkennung zu betreiben. Nebst Journalisten und Recherchespezialisten könnten ebenso OSINT- sowie KI-Experten in diesem Zentrum tätig werden, damit vollständige Analysen auch in diesen Bereichen erstellt werden können. Es besteht auch die Möglichkeit, Meinungsforschungsumfragen zu bestimmten Themen über Fake-News und Desinformation durchzuführen. Die Einladung von internationalen Experten und Organisationen und ein regelmässiger Erfahrungsaustausch mit ihnen wäre ebenfalls angebracht.

Privatwirtschaft

- Die Unterstützung der KMU durch staatliche Subventionen oder Steuererleichterungen im Bereich Cybersicherheit wäre eine empfohlene Massnahme im privatwirtschaftlichen Bereich. Somit wäre für die Schweizer KMU ein wirtschaftlicher Anreiz geschaffen, in die eigene Cybersicherheit zu investieren. Die Höhe der Subvention muss dabei den Umsatzzahlen der einzelnen Unternehmen angepasst werden, sodass die finanziellen Mittel auch gerecht verteilt werden können. Ferner kann auch das Versicherungsgeschäft im Bereich Cybersicherheit durch Subventionen oder Prämienverbilligungen gefördert werden. Durch vertiefte Prämienzahlungen und Steuererleichterungen wird den KMU ein zusätzlicher Anreiz geboten, in ihre Sicherheitsvorkehrungen zu investieren und sich gegen potenzielle Cyberangriffe zu schützen. Der effektive und nachhaltige Schutz der Schweizer KMU im Cybersicherheitsbereich hat ein strategisches Interesse für die Schweiz, zumal die KMU schon mehrmals als Rückgrat der Schweizer Wirtschaft bezeichnet wurden.

Kritische Reflexion und Ausblick

Eine vollständige Analyse der Schweiz im Bereich IW bedürfte einer kompletten Analyse der Schweizer Medienlandschaft. Zudem müsste eine repräsentative Umfrage mit einem bedeutenden Teil der Schweizer Bevölkerung aus allen Landesteilen durchgeführt werden. Ebenso müssten die Fähigkeiten der Schweizer Sicherheitsorgane insbesondere im Bereich Informations- und Cybersicherheit objektiv gemessen werden, damit auch dort konkrete Empfehlungen entstehen können. Erst nachdem dies erfolgt ist und dokumentiert wurde, könnten politische Massnahmen in beiden Parlamentskammern und in der Wandelhalle diskutiert werden. Aber auch die Öffentlichkeit müsste in solche Diskussionen frühestmöglich eingebunden werden, um mögliche zivilgesellschaftliche Initiativen zu fördern. ◆

Literaturverzeichnis

Der vorliegende Artikel ist eine Zusammenfassung der Bachelorarbeit des Autors. Die vollständige Arbeit kann unter folgendem Link heruntergeladen werden. In der Arbeit finden sich auch alle Quellen- und Literaturverweise.

Pustovit, K. (2023). Entwicklungsmöglichkeiten der Schweiz im Bereich Information Warfare nach 9 Jahren russisch-ukrainischem Konflikt. https://portal.fh-hwz.ch/Theses/openURL.aspx?id=2665&adr=127172