Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

The Federal Council

19 June 2024

Influence Activities and Disinformation

Report of the Federal Council
in Fulfilment of Postulate 22.3006
of the Committee on Security Policy of the National Council

Content

1. Introduction

1.1 Postulate 22.3006

In January 2022, the Security Policy Committee of the National Council submitted a postulate calling for an overview of the threat to Switzerland posed by disinformation campaigns.

Specifically, the Federal Council should set out in a report the extent to which Switzerland is affected by influence activities or disinformation campaigns. Furthermore, measures should be proposed to counter the threat. The postulate refers to the Federal Council's 2021 Report on Security Policy, which delved into the topic and explained that influence activities can sabotage political processes and undermine the population's trust in institutions. In view of the confrontations driven by power politics, the risk of being affected by such activities is also growing for Switzerland.

The Federal Council proposed the adoption of the postulate on February 23, 2022. The National Council adopted the postulate on March 9, 2022.

1.2 Relevance and Context

The security situation in Europe and in Switzerland’s vicinity has become more unstable, unclear and unpredictable. Tensions and rivalries between the major powers have increased. With Russia's military aggression against Ukraine, war has returned to Europe and the continent's security order has been permanently shaken. Old and new armed conflicts have flared up around Europe. In the Middle East, for example, these threaten to escalate further, with global consequences. Many societies in Western countries are increasingly polarized. Democratic values and international legal norms are under pressure worldwide. The way in which conflicts are fought is changing, shaped by power politics and technological changes. The information space plays an important role in conflicts, as can be seen in the war against Ukraine or the war between Israel and Hamas, and is a space for influence activities by various states.

Since the 2021 Security Policy Report, the use of means which are part of the repertoire of hybrid conduct of conflict, such as cyberattacks and influence activities, has increased. States that want to defend or change the existing balance of power by force are increasingly operating in the grey area between armed conflict and peace. The use of means of hybrid conduct of conflict is often complex and unpredictable. Actors who use such means can often plausibly deny their authorship. Open, democratic societies can be worthwhile targets for influencing their free debates and democratic processes. This can pose a threat to internal or external security. Accordingly, influence attempts by state or state-commissioned bodies should be recognized and countered better.

Influence activities in the information space in general, which include disinformation (see 2.1 for terms), are intensively discussed in politics and the media in many Western countries. They are often attributed substantial destructive potential. However, they are not a new challenge but are now exacerbated not only by shifts in power politics, but also by technological possibilities, the speed of information dissemination and the increasing role of companies – from social media platforms to "troll farms" – in the generation and dissemination of disinformation. The widespread use of social media and the increasing possibilities of generating and disseminating image, audio or video material using artificial intelligence (AI) exacerbate the challenge. Influence activities can also be accompanied and facilitated by cyberattacks. Growing social polarization is both breeding ground and target of influence activities.

It is above all state and state-commissioned actors who employ means and methods of influence and disinformation and often do so in a comprehensive, coordinated manner and with considerable resources. From a Swiss perspective and especially relevant in terms of state and security policy, are actors who aggressively advocate alternative values, norms and political systems and who want to undermine democratic institutions. The activities of Russia, but also China, are likely to remain of greatest relevance for Switzerland's security in the medium and long term.

Western states and alliances are also active in the information space and try to insert their views into political discussions in other countries. However, they are not to be considered as a threat to Switzerland in terms of security policy if they do not question or undermine the state order in Switzerland and the functioning of democratic state systems.

Current examples of influence activities in the information space can be observed around the war in Ukraine. To a global audience, Russian channels in social and online media offer an alternative interpretation, disinformation and the deliberate falsification of reality in Ukraine. The Kremlin, in turn, successfully controls through repressive measures the flow of information within Russia and in the occupied Ukrainian territories. China's influence activities worldwide and especially in Western states are also increasing in number. They are systemic and strategic, as many of such activities are instigated and directed by the Chinese Communist Party. They serve political and ideological interests that largely contradict widely accepted democratic principles. At the same time, China is tightening its own laws to protect itself against foreign influences on its own territory. Many other countries are also tightening their regulations to better control their national information space.

Switzerland, its society and its authorities are also increasingly affected by influence activities. Factors contributing to this include its commitment to international law and democracy, alongside a growing pressure to define its position within the global political power structure. As a state in the heart of Europe, as part of the Western community of values and the Western information space, and because of its strong economic and political interconnectedness, Switzerland has already been an indirect target of influence activities that target Western states in general for years. However, such activities are also increasingly aimed directly at Switzerland. There is also a risk that Switzerland's territory will be misused as a hub to carry out or finance influence activities against third countries or international organizations.

Switzerland needs to recognize systematic state or state-commissioned influence in the information space, to determine its intention and origin, and to react to it if necessary. Appropriately assessing the potential and functioning of influence activities is key to this.

1.3 Focus and Structure of the Report

This report focuses on the impact on Switzerland of influence activities that take place in the information space and are primarily carried out by state or state-commissioned foreign actors, as this is particularly relevant in terms of security policy. The report examines the impact of the issue on aspects of security and general state policy and thus how it directly and indirectly affects the functions, resilience and cohesion of the state and society.

The report presents the terminology and describes the goals, mechanisms, actors and effects of influence activities in the information space, including disinformation (chapter 2). It describes how other states, alliances and organizations deal with the issue (chapter 3). It then describes the threat situation for Switzerland, the extent to which it is affected, and specific Swiss characteristics, including case studies (chapter 4), and the current legal framework (chapter 5). It shows the work and responsibilities in Switzerland to date (chapter 6) as well as possible courses of action (chapter 7). A glossary at the end provides the common terms related to this topic.

2. Understanding Influence Activities and Disinformation

2.1 Definitions and Terms

Influence activities are particularly relevant in terms of security policy when they are perpetrated by states and are directed against the functioning of a state and a society and aim to undermine the democratic order of a state. This distinguishes influence activities from normal representation of interests, e.g. in the context of diplomacy or politics, which is intended to contribute to the formation of opinion in a legitimate way. This report focuses on influence activities in the information space, as opposed to cyberattacks or influence activities that use military means, such as sabotage or the deployment of troops abroad without state insignia. It focuses on foreign state or state-commissioned actors who are particularly relevant in terms of security policy; in contrast to activities by terrorist groups or economic actors with purely monetary goals.

There are no generally accepted precise definitions for the terms influence activity and disinformation. However, a basic understanding of the terms is common to most works. **Influence activities in the information space** are understood to mean various behaviours and strategies that aim to influence the perception, thinking and actions of individuals, groups and societies with manipulative intent. These activities can be carried out by both state and non-state actors. In addition to disinformation, the tools include other means of influencing the information space, such as the deliberate omission or reinterpretation of facts, the manipulation of visual content, the use of false profiles in social media, or censorship.

Disinformation describes misleading or completely fabricated information that is deliberately used to influence public opinion and political processes, undermine the credibility of institutions and the media, or sow doubts about the reliability of information.[1] The EU and NATO, which use similar definitions, understand disinformation in the broader sense to mean information that is verifiably false or misleading and that is created, pre-formulated and disseminated for profit or with the conscious intention of deceiving the public.[2] Different actors with different motives can create and disseminate disinformation. Not every type of disinformation is an influence activity or even relevant to security or general state policy.

Both influence activities and disinformation are largely characterized by the fact that false information is disseminated intentionally, i.e. with the intention of deceiving, in contrast to (bona fide) false or misinformation (for this and other terms, see the glossary). Disinformation or influence activities therefore do not include errors and misinformation made in good faith, nor satire, parody or biased information and comments clearly identified as such.

2.2 Objectives and Methods

Influence activities carried out by states are often directed against open and democratic societies that are based on an honest competition of ideas on a recognized basis of facts and where the free dissemination of information – even false information – is a fundamental right. The aim of such activities in the information space is usually to influence public opinion and political or other decisions in order to anchor a certain point of view in a target group and to weaken the credibility of the opposing party. The aim of these influence activities is to unsettle, frighten, upset or divide the target population. Trust in state institutions is to be undermined.

Information content is delivered to an audience from one or more sources via various information channels. Influencing actors usually define this audience in advance and choose the context and timing of the information activities to achieve the greatest possible effect. They can coordinate several activities as part of an operation. Figure 1 illustrates the elements of preparing such a coordinated action and the subsequent steps. Not all activities are necessarily planned well in advance or in detail; and achieving the intended goal is never guaranteed, even with precise planning and significant resource commitments.

An understanding of target groups is particularly important for influence actors. For individuals, for example, certain character traits such as vanity or genuine helpfulness play a role, and for groups, certain socio-demographic or collective characteristics such as national traumas or social fault lines can be exploited. It can be assumed that authors of influence activities cannot always reach their target audience precisely or precisely calibrate their content. However, disinformation already has an effect when they sow doubts about established facts or official information without the specific disinformation content being considered true. There are also signs that influence activities use a variety of different and sometimes contradictory narratives to increase the chances of success with different target groups. Influence activities are risky, and revealing their authorship can be counterproductive, which is why often considerable efforts are undertaken to conceal it.

Even if disinformation has been identified and refuted as such, it often keeps spreading. Psychology has shown that frequently repeated statements are more likely to be believed, regardless of the truth of their content (illusory truth effect).[3]

[1] Federal Office of Communications, Report "Desinformation in der Schweiz 2021" *(Disinformation in Switzerland 2021).*

[2] See <https://commission.europa.eu> and <https://www.nato.int>.

[3] Catherine Hackett Renner, *Validity effect,* in: Rüdiger F. Pohl (Ed.), "*Cognitive illusions",* Psychology Press (Hove, UK: 2004), p. 201–213.

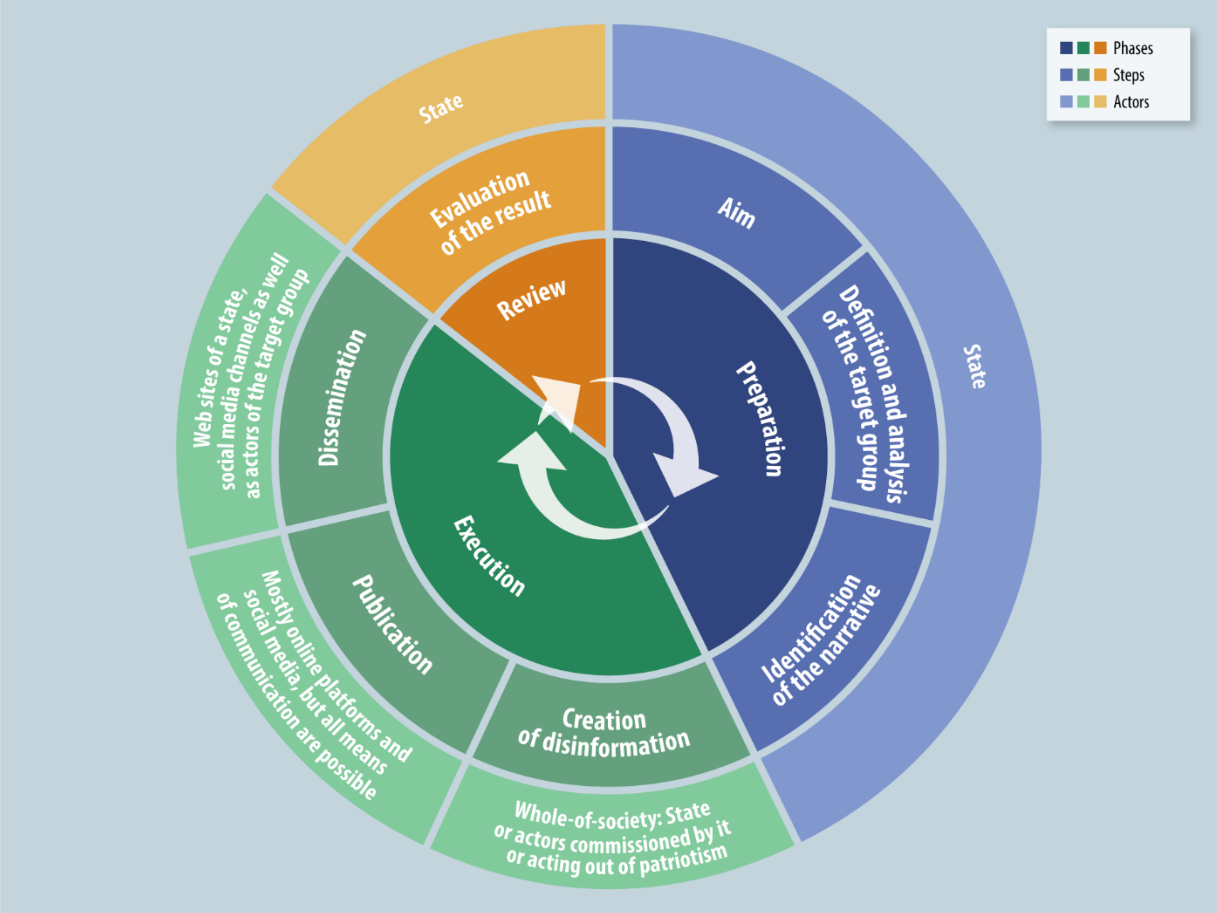
Phases
Steps
Actors
State
Evaluation of the result
Review
Aim
State
Definition and analysis of the target group
Preparation
Identification of the narrative
Creation of disinformation
Execution
Publication
Dissemination
Web sites of a state, social media channels as well as actors of the target group
Mostly online platforms and social media, but all means of communication are possible
Whole-of-society: State or actors commissioned by it or acting out of patriotism

Figure 1: Exemplary process and actors of a disinformation operation by a state

Another method is to visually clone well-known media portals, fill them with disinformation and thus benefit from the credibility and popularity of these media outlets. Research by the German press and the NGO DisinfoLab and Qurium uncovered Operation "Doppelgänger" at the end of 2022. It had produced more than 60 fake news sites that imitated major international media (Le Monde, The Guardian, Spiegel, etc.), as well as more than 1,600 accounts and several hundred fake pages on social networks. According to Meta's security report of August 29, 2023, the operation was used to spread disinformation in Russia's interest about the war against Ukraine.[4]

Furthermore, cyberattacks can facilitate influence activities, when acquired sensitive or classified information is subsequently passed on to a target audience in original or manipulated form as part of an influence activity ("hack and leak").

2.3 Actors

Influence activities include many possible actors, as figure 1 illustrates, including government bodies, companies such as platforms or media companies, and individuals, such as media users; knowingly and possibly commissioned, or unknowingly. This complicates coordination and control over the process for influence actors, and also contributes to such activities not necessarily succeeding, even with substantial resource investments.

Political and authentic or seemingly authentic civil society actors can be vehicles for influence activities. For the dissemination of its view, Russia, for example, often uses seemingly apolitical institutions and associations as a front, as well as certain Russia-friendly parties and politicians in Western states.

[4] Meta, Meta’s Adversarial Threat Report, Fourth Quarter 2022, 23 February 2023, <https://about.fb.com/news/2023/02/metas-adversarial-threat-report-q4-2022> (retrieved on 21 February 2024).

The connection to or funding by the Russian state may not be obvious to these participants. The Kremlin created a well-disposed network of European politicians from across the political spectrum through party donations, conferences and invitations to Russia. China, meanwhile, covertly exploits the Chinese diaspora community to defend and promote its interests. It also exerts influence by using non-Chinese key actors for its purposes, with or without their knowledge. The media, politicians, administrations, the private sector and entrepreneurs, universities and associations can be the targets of such efforts.

Increasing digitalization and a wide range of technological means make information accessible to a wide audience cheaply and transnationally. Users can not only be recipients of information but can also share, comment and "like" digital content, thus helping disinformation reach a wider audience – unconsciously or consciously, for example to generate clicks and attention. In social media in particular, it is difficult to recognize disinformation and its authorship at all, or even in time. The EU has analysed that primarily images and videos are used to influence people.[5] Russia, for example, intensively uses digital information and communication tools to spread disinformation. In addition to social media, these include the Russian state foreign broadcasters Russia Today (RT) and Sputnik, which report in over 30 languages worldwide, including German and French.

The use of manipulative methods and technologies can also be facilitated by private actors in the "influence-for-hire" industry, which market various services and software products online to support influence activities. For example, the Israeli company "Team Jorge", which was exposed in 2022, offered to manipulate elections, including through disinformation.

Inauthentic accounts of so-called internet trolls and bots can launch debates, question statements or spread rumours on social media and online forums. Real people acting on behalf of states who, under false identities, pretend to be normal users, or so-called "social bots", can generate many posts and thus create the false impression that many people hold a certain opinion. Computer programs can, for example, automatically publish standardized answers to certain topics in forums.

At the end of August 2023, the company Meta identified a network of 7,704 fake accounts, 954 pages and groups on Facebook and 15 accounts on Instagram that had spread disinformation on behalf of China. The network primarily spread positive comments about China and the Xinjiang region, where the Chinese state is carrying out extensive repression against the Uighur minority, as well as messages targeting the United States, Western governments, and journalists and scientists in China critical of the Chinese government.[6]

Therefore, digital platforms play a key role in the spread of disinformation. Often non-transparent algorithms on platforms and search engines can recommend content based on the preferences and interests of users and place widely shared content more prominently. If someone has already interacted with disinformation or has a user profile that is susceptible to it, similar content is often suggested. This shows that the openness of the internet and the low technical access barrier, combined with the absence of journalistic and editorial selection of information, can lead to an increased spread of disinformation.[7] Disinformation is also spread on digital platforms and media portals because it generates clicks and thus revenue for the companies involved. Real or fictitious media organizations spread insufficiently verified content, for example with sensational headlines or misleading preview images ("clickbait").

Terms and conditions and moderation services vary considerably between platforms. In response to certain restrictions, such as the EU banning of RT and Sputnik or the blocking of many of their fake social media accounts, Russia is increasingly relying on alternative channels on the Internet, such as slightly modified internet addresses or newly created platforms. Since the beginning of the war in Ukraine, there

[5] EEAS, Report on FIMI Threats, February 2023, p.5 <https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf> (retrieved on 21 February 2024).

[6] The Guardian, Meta closes nearly 9,000 Facebook and Instagram accounts linked to Chinese 'Spamouflage' foreign influence campaign, 29 August 2023; <https://www.theguardian.com/australia-news/2023/aug/30/meta-facebook-instagram-shuts-down-spamouflage-network-china-foreign-influence> (retrieved on 23 February 2024).

[7] See *Saurwein/Spencer-Smith,* Inhaltsregulierung auf Internet-Plattformen. Optionen für verantwortungsorientierte Governance auf nationaler Ebene *(Content regulation on Internet platforms. Options for responsibility-oriented governance at national level)*, p. 42.

has been an increase in Russian propaganda content in European languages on lightly regulated, non-Western platforms such as TikTok and Telegram.

The rapid development and spread of AI threaten to increase the potential for influence activities dramatically, both quantitatively and qualitatively. AI automates many of the processes necessary to develop and spread disinformation. One example is deep fakes. Deep fakes are videos, images or audio files that have been manipulated using AI, often with little effort and time, to falsify people or events in a deceptively realistic way. These can be used on all common channels, especially unmoderated social media. Tools such as Large Language Models (LLM) make it easier to use user accounts under false identities and to imitate social movements ("astroturfing"). As they use increasingly better language models, they are becoming increasingly difficult for people, regulators, and supervisory authorities to recognize as artificially generated.

2.4 Possible Effects

All influence activities are based on the premise that activities in the information space can have an influence on people's thoughts, discourses and actions. Influence activities within the information space can negatively affect trust in institutions, as well as free opinion and decision making, and thus democratic processes, national security and the states' capacity to act effectively – even if these activities only reach a small segment of the population. A basic distinction must be made between short, medium and long-term effects. For example, in the short term, the opinion making process on a popular vote; in the medium term, for example, the tone, character and degree of polarization in a country's political discourse; and in the long term, for example, the trust in institutions.

It is difficult to measure the exact impact of influence activities, for example the effects of influence activities by states using social media.[8] Therefore, in research and media, possible effects, as well as which constellations of disinformation content, timing, ease of dissemination and contextual factors favour them, are assessed differently. Especially relevant are the effects of sustained, possibly coordinated influence activities and disinformation, not of singular activities.

Influence activities and disinformation can contribute to a sustained damage of trust in politicians – public figures in general –, the media, institutions, and information itself. Influence activities can impair the free formation of will and opinion in democratic processes. Those affected can turn away from politics because their trust in information and processes has eroded. A lack of trust in democratic institutions and processes can render communication and finding compromises across political divides more difficult, as the common factual basis, a foundation for political discourse, is called into question. Influence activities can, for example, undermine trust in the police and law enforcement authorities by creating the impression that these authorities investigate one-sided, act arbitrarily or have been "infiltrated". In the worst case, this can lead to the radicalization of those affected.

The structural and lasting impact of influence activities can in turn prepare the ground for possible short-term effects, such as the mobilization for political action or the use of violence. In addition, influence activities and the spread of disinformation sometimes limit the freedom of action of authorities by tying up resources, especially in times of crisis and uncertainty.

Various examples show influence activities by other states and their effects on the resilience of democratic institutions. Russian accounts on Facebook and X/Twitter spread disinformation around the British Brexit referendum and the 2016 US presidential election.[9] France was the target of Russian influence activities during the 2017 presidential election as sensitive material was leaked to discredit the leading candidate Emmanuel Macron.

Content disseminated by Russian actors includes, for example, migration, the departure from traditional family structures, criticism of arms deliveries to Ukraine, or discriminatory police violence. These topics are also reflected in authentic opinions, fears and demands in society. It is therefore difficult to draw a precise line between what arises from the free formation of opinion or from manipulation and deliberate

[8] Jon Bateman, Elonnai Hickok et al, Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research, 28 June 2021, <https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research-pub-84824> (retrieved on 5 April 2024).

[9] *Bayer et al.,* Disinformation and propaganda.

deception and is therefore exaggerated. In certain policy areas, influence activities in the information space go hand in hand with other means of the hybrid conduct of conflict; for example, when the Belarusian regime purposefully helped migrants from the Middle East cross the border into Poland and Lithuania in autumn 2021. This was accompanied by disinformation in Russian media about the alleged complete dysfunctionality of European asylum and migration systems. However, Russia is currently barely able to significantly influence the majority opinion of society and political decisions in Western countries – for example, regarding the war in Ukraine.

Disinformation during the COVID-19 pandemic appealed to scepticism towards government agencies and to emotions and fears. Disinformation can also lead people to ignore health advice from official bodies and incur health risks. It is therefore relevant to security policy and can also affect the economic and financial situation of a country. Such effects are also conceivable in the short term. An AI-generated image of an allegedly burning US government building, for example, circulated within minutes on Facebook and X/Twitter in May 2023, including the accounts of the Russian RT. A short-term daily low on US stock markets that day is partly attributed to this.[10]

Influence activities and disinformation can also impact peacebuilding and humanitarian efforts. UN peacekeeping missions in Mali, the Central African Republic and the Democratic Republic of Congo are or have been affected by disinformation. In the Central African Republic, online disinformation, including fake video footage, accused four UN employees of supplying weapons to rebels and called for violence against the mission.[11] Such disinformation contributes to resentment among the local population, which can escalate into violence. This endangers the personnel of international missions and the promotion of security and peace in the country.[12] Humanitarian organizations such as the International Red Cross can also be affected by such activities.

3. Assessment and Management in International Comparison

In recent years, an increasing number of states and international organizations (e.g. NATO, EU) have recognized influence activities in the information space as a challenge to their security. Those who feel particularly affected are somewhat more advanced in their measures – such as the USA, the United Kingdom, France or Germany due to their international presence, or Australia, the Nordic and Baltic states due to their geographical proximity to China or Russia. Due to the transversal effects, efforts are also being made at the international level to increase cooperation and coordination.

In principle, many countermeasures have so far only been tested to a limited extent and their design and effectiveness depend heavily on the national context. The following approaches are non-exhaustive.

3.1 Strategic Assessment

Australia, Germany, France, the Netherlands, Canada, Austria, the United Kingdom and the USA consider influence activities and disinformation a strategic threat; the Netherlands explicitly as a threat to national security.[13] Germany (National Security Strategy of June 2023) and France *(Actualisation stratégique 2021)* highlight the threat to democratic decision-making processes. The USA and the United Kingdom also emphasize the risk of undue influence on the free formation of political opinion through disinformation, considering the combination with new technologies and *big data* to be particularly worrying *(US 2023 Annual Threat Assessment; UK Integrated Review of Security, Defence, Development and*

[10] The New York Times, An A.I.-Generated Spoof Rattles the Markets, 23 May 2023, <https://www.nytimes.com/2023/05/23/business/ai-picture-stock-market.html#:~:text=Fake%20news%2C%20real%20market%20drop,investor%20fears%2C%20sending%20stocks%20tumbling> (retrieved on 21 February 2024).

[11] Albert Trithart, Disinformation against UN Peacekeeping Operations, International Peace Institute, November 2022, p. 3, <https://www.ipinst.org/wp-content/uploads/2022/11/2212_Disinformation-against-UN-Peacekeeping-Ops.pdf> (retrieved on 21 February 2024).

[12] Thus 75% of the interviewed UN peacekeepers indicated in a poll that disinformation had an impact on their security. See Ibid., p. 13.

[13] The Security Strategy for the Kingdom of the Netherlands, 3 April 2023, <https://www.government.nl/binries/government/documenten/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands/Security+Strategy+for+the+Kingdom+of+the+Netherlands.pdf> (retrieved on 21 February 2024).

Foreign Policy 2021). These states see a particular need for action in the early detection and strengthening of the resilience of institutions and society. Germany intends to develop two strategies: one to increase the ability to act against hybrid threats and one to deal with disinformation. Austria focuses on establishing and expanding civil-military cooperation formats and intensifying cooperation with other EU member states.

Based on its 2022 Strategic Compass for Security and Defence, the EU developed a toolbox to fight against foreign interference and information manipulation (FIMI). This includes improving situation assessment and early warning, strengthening societal resilience, and regulatory and restrictive measures within the framework of geographical sanctions regimes. By 2024, all missions and operations under the EU's Common Security and Defence Policy should be able to counter information manipulation and foreign influence. According to its 2022 Strategic Concept, NATO will invest in its ability to prepare for hybrid threats such as disinformation and influence activities. Alarmed by the increasing risks to international peacekeeping missions, the UN's awareness has also increased in recent years. In July 2022, the UN Security Council expressed concern about the increasing impact of disinformation on peacekeeping missions. The Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression devoted her last two reports to aspects of disinformation.[14]

3.2 Situation Monitoring and Early Detection

Various states have created institutions specifically for early detection. In July 2021, France founded the organization Viginum *(Vigilance et Protection Contre les Ingérences Numériques Etrangères).* Based on publicly available sources, Viginum analyzes patterns of foreign influence activities, particularly in the run-up to elections. In 2022, Sweden established a so-called psychological defence agency[15] with the aim of identifying, analysing and combating foreign influence activities in the information space and strengthening the resilience of the population. In the United Kingdom, a directorate in the Foreign Ministry analyses and conducts research based on publicly available information and formulates appropriate strategies and countermeasures. A *Defending Democracy Taskforce* focuses specifically on the early identification of threats to elections through influence activities in the information space. In the USA, the *Global Engagement Center* is monitoring the situation and confronts with facts narratives spread by Russia.[16]

In 2018, the seven leading industrial nations (G7) set up the *G7 Rapid Response Mechanism* under the leadership of Canada to analyse the information space and identify threats. The mechanism provides for joint measures and coordination. Australia, New Zealand, the Netherlands, NATO and Sweden are observers. The *Rapid Alert System* in the EU's European External Action Service (EEAS) promotes the exchange of information between member states. EUvsDisinfo,[17] an information platform of the EU, analyses and publishes current narratives to raise awareness among the population. In its second report on FIMI in January 2024, the EEAS identified 750 individual incidents of influence activities for the period between December 2022 and November 2023.[18]

3.3 Resilience through Raising Awareness, Education, and Media Literacy

Democratic governments and researchers see the strengthening of resilience and a whole-of-society approach as the most important but also challenging measures for countering influence activities in the information space. Many initiatives particularly focus on raising awareness in society, strengthening media literacy among the population and improving media quality.

[14] OHCHR, Disinformation and freedom of opinion and expression during armed conflicts, 12 August 2022, <https://www.ohchr.org/en/documents/thematic-reports/a77288-disinformation-and-freedom-opinion-and-expression-during-armed>; OHCHR, Freedom of expression and the gender dimensions of disinformation, 7 August 2023, <https://www.ohchr.org/en/calls-for-input/2023/report-freedom-expression-and-gender-dimensions-disinformation>.

[15] Myndigheten för psykologiskt försvar (Psychological Defence Agency),

[16] See <https://www.state.gov/disarming-disinformation/#reports>.

[17] See <https://euvsdisinfo.eu/de/>.

[18] European External Action Service, 2nd EEAS Report on Foreign Information Manipulation and Interference Threats, January 2024, <https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en> (retrieved on 5 March 2024).

Germany is establishing a centre for strategy, analysis and resilience, in which the interior, foreign and defence ministries are represented. Sweden is cooperating with civil society organizations, research institutions, media, and municipalities to counter influence activities in the information space and to raise awareness among the population and invests 1.2 million Euros[19] annually in research. The United Kingdom has made efforts in recent years to strengthen the population's media literacy through regulatory initiatives and campaigns. Similar work can be observed in Australia.

The *European Digital Media Observatory* (EDMO), an EU-funded network, brings together actors such as media, platforms, civil society and research, analyses disinformation campaigns, monitors measures taken by the tech industry and strengthens the media literacy of the population. EDMO is involved in the revision and evaluation of the EU's *Strengthened CoP* (see 3.4).

Other joint initiatives by states in which Switzerland is also involved aim to strengthen the protection of privacy and access to reliable information as well as protecting journalists and media professionals, for example through the *Media Freedom Coalition,* the coalition for internet freedom and the protection of human rights *(Freedom Online Coalition)* or the International Partnership for Information and Democracy.

3.4 Regulation and Sanctions

Numerous states have taken initiatives to regulate digital platforms. The approaches cover a wide spectrum from state regulation to co-regulation and self-regulation. The legislative approaches focus on removing content deemed harmful or labelling it, transparency regarding advertising, strengthening the rights of users, and supporting research. The USA has established an authority on the basis of the 2020 *National Defense Authorization Act,* the *Social Media Data and Threat Analysis Center,* which ensures coordination with social media platforms.

At EU level, a new regulation came into force in August 2023 with the *Digital Services Act* (DSA), which the platforms implemented in part independently. The Digital Services Act is intended to prevent the spread of illegal content in the digital space and protect the fundamental rights of users. Disinformation is partially covered when it comes to hate speech and other offenses of illegal expression or threats to public security. In the context of the war between Israel and Hamas, the European Commission formally requested information from Meta and TikTok in October 2023 on their measures against the spread of disinformation. It also accelerated the monitoring and enforcement of the Digital Services Act, including a coordination mechanism between member states against the spread of illegal content.

The European Commission wants to combat disinformation on social media with a voluntary code of conduct for technology and advertising companies. 40 companies have so far signed this *EU Code of Practice on Disinformation;* due to a lack of effectiveness, it has been revised into the *Strengthened Code of Practice* and includes a permanent task force.[20] The UN is also relying on a code of conduct to counter the digital spread of disinformation. This is intended to call on state and non-state actors to take action against disinformation and respect human rights. Some countries are also choosing direct regulatory approaches. For example, the Norwegian government has proposed a draft law that would criminalize participation in influence activities on behalf of foreign intelligence services. Various countries – such as Brazil, Cambodia, Croatia, France and Kenya – have passed laws against online disinformation in connection with elections. Many of these laws were accompanied by concerns and protests about freedom of expression and freedom of the media and were withdrawn in several other countries.

The toolbox developed by the EU *(FIMI Toolbox;* see 3.1) includes, within the framework of geographical sanctions regimes, restrictive measures against companies and individuals responsible for influence activities in the information space. In the context of the war against Ukraine, the EU and its member states have imposed sanctions against Russian individuals and entities (entry bans, freezing of assets, prohibition on the provision of funds or economic resources, withdrawal of licenses). These include five RT channels and Sputnik. On July 28, 2023, the EU sanctioned a further seven individuals and five entities

[19] Jean-Bapiste Jeangène Vilmer: Effective State Practices Against Disinformation: Four country case studies. Hybrid CoE Research Report 2 (July 2021), p. 12.

[20] Members of the task force are the signatories, the European Regulators Group for Audiovisual Media Services, European Digital Media Observatory and the European External Action Service. It is chaired by the European Commission.

for information manipulation.[21] On May 30, 2023, and February 22, 2024, the EU imposed sanctions against companies and individuals from Moldova for destabilizing the republic, including through disinformation.[22]

Several countries, including the United Kingdom, the United States and Australia, have imposed sanctions on influence agents and their platforms. Leading Western social media platforms such as Facebook, YouTube and X/Twitter have, to varying degrees, restricted access to and the distribution of content from Russian state-affiliated sources.

3.5 Responsibilities, Coordination and Communication

Since influence activities in the information space affect many subject areas and jurisdictions, responsibilities in governments are regulated very differently and span many ministries, requiring coordination.

In France, the Prime Minister's Office, which is also where Viginum is associated, is in the lead. A scientific ethics committee monitors the organization's activities. In Germany, the Ministry of the Interior is responsible for matters of disinformation and influence. It coordinates an interdepartmental working group. In Sweden, the Psychological Defence Agency is part of the Ministry of Defence. The Baltic states also want to explicitly address influence activities and disinformation in a whole-of-state approach, including by promoting media literacy among the population and the integration of minorities, particularly Russian minorities. In the United Kingdom, the Foreign Office coordinates the activities, while various other governmental departments deal with the issue from their perspective. Similarly, in the USA, the *Global Engagement Center* is affiliated to the State Department and is tasked with coordinating the government's efforts to combat disinformation. In the EU, more than 40 EEAS staff advise the Union and its member states on how to deal with illegitimate influence and disinformation by foreign actors, in addition to producing annual reports.

Migration is a recurring theme of disinformation, and migration flows can be instrumentalised for hybrid conduct of conflict. In view of this, in 2021 the European Commission proposed a regulation to address situations in which a third country triggers irregular migration flows into the EU to destabilise it or a member state.[23]

Various states have increased strategic communication to counteract influence activities in the information space, for example within NATO. Strategic communication covers a bundle of coordinated communication activities that are intended to convey and legitimize one's own goals, interests and actions and thus counter opposing narratives. The EU has defined a specific unit specifically for strategic communication within the EEAS. NATO’s efforts are supported by an independent competence centre, the *NATO Strategic Communications Center of Excellence.*

[21] European Council, Media release, Information manipulation in Russia’s war of aggression against Ukraine: EU lists seven individuals and five entities, 28 July 2023, <https://www.consilium.europa.eu/en/press/press-relea-ses/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-indivi- duals-and-five-entities/> (retrieved on 21 February 2024).

[22] European Council, Media release, Republic of Moldova: 7 individuals listed for their destabilising actions and for undermining the territorial integrity of Ukraine, 30 May 2023, <https://www.consilium.europa.eu/en/press/press-releases/2023/05/30/republic-of-moldova-7-individuals-listed-for-their-destabilising-actions-and-for-undermining-the-territorial-integrity-of-ukraine/>; European Council, Media release, Republic of Moldova: six individuals and one entity listed for undermining the rule of law, stability and security in the country, 22 February 2024, <https://www.consilium.europa.eu/en/press/press-releases/2024/02/22/republic-of-moldova-six-individuals-and-one-entity-listed-for-undermining-the-rule-of-law-stability-and-security-in-the-country/> (retrieved on 18 March 2024).

[23] This mainly against the background that Belarus, in the autumn of 2021, fostered irregular migration to Poland and Lithuania; European Commission, Directorate-General Migration and Home Affairs, Proposal for a Regulation addressing situations of instrumentalization in the field of migration and asylum,2021/0427/COD, <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52021PC0890> (retrieved on 5 March 2024).

4. Switzerland's Exposure

4.1 Threat Situation

With its system of direct democracy, in which the population regularly takes political decisions, with some potential social and political fault lines, as well as being a foreign policy actor and host to numerous international organizations, Switzerland can be a convenient target for influence actors. As a state in Europe and part of the Western community of values, and because of its strong international economic and political interconnectedness, Switzerland has long been an indirect target of general influence activities aimed at Western states. However, it is increasingly also directly targeted by specifically tailored activities. Nevertheless, there is no evidence that federal votes have been a direct target of influence activities.

For Switzerland, the main presumptive authors in relation to influence activities are Russia, but also China.[24] Since Russia placed Switzerland on its list of "unfriendly states" after Switzerland had imposed sanctions in connection with the war against Ukraine, Russian disinformation activities tailored to Switzerland have increased, most recently in the context of the High-Level Conference on Peace in Ukraine hosted by Switzerland in summer 2024. Even if Russian foreign media do not operate Switzerland-specific platforms, their multilingual content can reach the Swiss population. However, the Federal Council ultimately considers their reach to be limited. Russian influence activities are likely to intensify when political debates or the outcome of political processes in Switzerland, such as public votes, are of particular importance to Russia's interests. These can include debates about the supply of energy, neutrality, sanctions, support for Ukraine or the possible use of frozen Russian central bank assets.

The issue is increasingly noticed and discussed in Swiss politics, media, and society. The Swiss population is and feels confronted with disinformation. The 2021 internet usage survey by the Federal Statistical Office shows that almost half of the population (45 %) say they have seen questionable information on news sites or social networks. Consequently, half of media users either believe they have not seen any questionable content or have not recognized it as such. According to the report "Disinformation in Switzerland 2021"[25] commissioned by the Federal Office of Communications, almost half of those surveyed consider disinformation to be a major or very major problem. According to the report, disinformation poses a major problem for the trust in the media, politics, and authorities, as well as for social cohesion. To what extent influence activities have actually already led to such effects is difficult to determine. The negative consequences regarding social polarization, the rules-based international order and international peacebuilding (see 2.3) also affect Switzerland’s political and economic interests.

It is worth emphasizing the potential threat posed by influence activities to Switzerland as a foreign policy actor and as the host of many international organizations. With its law on the supervision of associations and foundations, in which self-control plays an important role, the risk of influence activities being financed via Switzerland could increase. For example, Vladimir Yakunin, who is part of Putin's close circle of friends, financed his influence and lobby organization "Dialogue of Civilizations" through a network of foundations in Switzerland. The establishment of institutes described as scientific, or of internet portals critical of the media, which hope to acquire a particularly credible appearance by virtue of their location in Switzerland, can also be observed.

4.2 Case Studies

Two well-known examples illustrate the content, narratives and processes of such influence activities and their impact on Switzerland: disinformation surrounding the Spiez laboratory in 2018 and a fake energy poster in 2022. They show how Switzerland became a direct target in the context of larger, Europe-wide campaigns.

In March 2018, after Russian agents had poisoned former Russian spy Sergei Skripal and his daughter with Novichok in the United Kingdom, the Spiez laboratory came into the global spotlight because, like

[24] Report on Security Policy of the Federal Council 2021, BBl 2021 2895 (German-language version), and Supplementary Report of September 2022, BBl 2022 2357 (German-language version).

[25] Vogler, D., Schwaiger, L., Schneider, J., Udris, L., Siegen, D., Marschlich, S., Rauchfleisch, A., Eisenegger, M. (2021), Falschinformationen, Alternativmedien und Verschwörungstheorien – Wie die Schweizer Bevölkerung mit Desinformation umgeht (*False Information, Alternative Media, and Conspiracy Theories – How the Swiss Population Deals with Disinformation*), Report of the Federal Office of Communications.

other laboratories, it analysed samples related to the incident within the framework of the Organization for the Prohibition of Chemical Weapons (OPCW). Russian state, state-sponsored and non-state actors attempted to undermine the credibility of the laboratory and of the results of its analysis on social media and through state-controlled media, while attributing responsibility for the poison attack to other actors. Russian Foreign Minister Sergei Lavrov claimed that the Spiez laboratory had not identified Novichok samples as such. Many Western media reported Lavrov's statement. The Federal Council and the Spiez laboratory unambiguously refuted his statement. Russian troll factories such as the *Internet Research Agency* were involved in spreading the statement and related disinformation via social media platforms such as X/Twitter and Facebook. Two Russian nationals were arrested in the Netherlands for attempted espionage against the Spiez laboratory. The Russian actions against the Spiez laboratory and the OPCW were primarily intended to distract from Russia's role, but accepted a reputational damage to the Spiez laboratory and thus to Switzerland.

In autumn 2022, a fake federal campaign poster, which advertised a reward of 200 francs for denouncing neighbours who overheated their homes, circulated on the social networks X/Twitter and Telegram. At the time the photomontage was published, Switzerland was intensely debating a looming energy shortage in connection with the war in Ukraine. On September 6, 2022, four days before the disinformation was first published, a Swiss daily newspaper published an article about proposed new regulations that would threaten residents who heated their homes to over 19 degrees centigrade with fines or prison sentences. The same day, international media, including the German-language RT, replicated this report. Within hours of its publication online, the photomontage spread rapidly across various social media and online platforms, including through inauthentic accounts attributed to the Russian influence network.

The conveyed narrative implied that the democratic system and the rule of law were dysfunctional and that autocratic conditions prevailed in Switzerland. The population was to be unsettled and divided. In addition, the case tied up resources within various authorities. More than 80 people called the General Secretariat of the Federal Department of the Environment, Transport, Energy and Communications, whose telephone number appeared on the photo montage, wanting to respond to the alleged call for denunciations. However, the isolated disruption of the work of the federal administration had no drastic effects and the activity did not reach a critical mass in society.

4.3 Specific Characteristics and Resilience of Switzerland

Switzerland possesses some characteristics that tend to reduce its exposure to influence activities and disinformation. However, the picture is nuanced.

The small size of the country and its media landscape, the high standard of living, the good level of education, the above-average trust in state institutions and the political competence, based among other things on the frequent referendums, all play part in strengthening the resilience of the country and its institutions. According to the report "Disinformation in Switzerland 2021", which cites various comparative studies, Switzerland as a country is structurally more resilient than many others. The less polarized society and the media landscape with many high-quality media are an important explanation for this, or a manifestation of it. The interaction of public and private media as well as the multi-party system with its consensus-based politics strengthen Switzerland's resilience against polarization and populism on the internet in international comparison.[26] Another study considers Switzerland to be less affected by fake news in comparison to the rest of Europe due to its low geopolitical relevance and linguistic diversity.[27]

However, Switzerland's direct democracy and federal structure not only represent strengths, but also a possible vulnerability to disinformation. The large number of votes at all levels of government offers actors the opportunity to exert influence on a case-by-case basis. However, the authorities organising elections and referendums at the various levels of government have acquired a great deal of experience

[26] According to Tobias Keller, communications and media scientist at the research institute gfs.bern, who has contributed to the study Digitization of the Swiss Democracy. Urs Bieri et. al.: Digitalisierung der Schweizer Demokratie. Technologische Revolution trifft auf traditionelles Meinungsbildungssystem *(Digitization of the Swiss Democracy. Technological revolution meets traditional system of opinion-formation),* Zürich, 2021.

[27] Humprecht, Edda, et. al.: Resilience to online disinformation: A framework for cross-national comparative research. In: International Journal of Press/Politics, Vol. 25, 2020, p. 493-516.

through the numerous votes. They cooperate closely and regularly exchange information in various institutionalised formats,[28] in specific bodies[29], and at the international level.[30] The VOX studies carried out by the opinion research institute gfs.bern showcase the population's trust in the information provided by the Federal Council in newspaper articles (81%), in television programmes (72%) and particularly in the context of votes, through the Federal Council's explanatory brochure (83%).

The transparency provisions that came into force in 2022 stipulate a ban on political actors accepting anonymous donations as well as donations from abroad (see article 76h of the Federal Law on Political Rights). These bans should also provide a certain degree of protection against foreign influence activities in the information space.

If, in addition to these structural factors, the issue of influence activities at the individual level is considered, several indications suggest that the Swiss population’s resilience with regard to disinformation could decrease in the future. The population does have a comparatively high level of competence in civics. However, a study found that Swiss respondents had rather low levels of media literacy, slightly lower than in a German comparative study. For example, many respondents found it difficult to determine the intention of the communication of a media article (as information, commentary or advertising), which is probably key to assess disinformation. 73% of respondents stated that they were completely or partially overwhelmed by the amount of information available.[31] Media literacy and thus resilience to influence activities tends to be higher among individuals with a greater degree of interest in news, political participation, use of digital and traditional media, and trust in Swiss media in general. Older people are a particularly vulnerable group to disinformation because, regardless of their level of education, their media literacy is lower than that of other age groups.[32]

According to recent findings, the Swiss population nevertheless considers itself to have slightly above-average digital media literacy compared to other countries. According to the 2021 omnibus survey on internet usage,[33] the Swiss population's *self-assessment* regarding digital skills is in the upper third compared to other countries: almost 78% of the population say they have basic or advanced knowledge.[34] This shows a discrepancy between self-assessment and the actually measured level of skills when it comes to media literacy.

The number of people in Switzerland who do not consume traditional news broadcasts is increasing.[35] In 2023, only 22% of the 18- to 24-year-olds said they got their information directly from a newspaper publisher's website or app, compared to 53% in 2015. The rest come into contact with information via

[28] Staatsschreiberkonferenz SSK (Conference of the cantonal record keepers).

[29] For example, the election and voting officer meeting of the federal government and the cantons, which has been organised annually by the Federal Chancellery since 2012.

[30] See among others: Elections in times of crisis: Conference of the Council of Europe in Bern, https://www.parlament.ch/en/services/suche-news/elections-in-times-of-crisis> (retrieved on 27 February 2024) / Conférence parlementaire – Les élections en temps de crise (Berne, 9 et 10 mai 2023) <https://pace.coe.int/fr/pages/bern-elections-conference> (retrieved on 27 February 2024).

[31] Jan Fivaz, Daniel Schwarz, Die Medienkompetenz der Schweizer Bevölkerung. Eine repräsentative Pilotstudie für die deutsch- und französischsprachige Schweiz *(Media literacy of the Swiss population. A representative pilot study for German- and French-speaking Switzerland),* 2022, p. 15, 49-51, <https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/elektronische_medien/Zahlen%20und%20Fakten/Studien/schlussbericht-die-edienkompetenz-derschweizer-bevoelkerung.pdf.download.pdf/Bericht%20Medienkompetenz%202022%202.pdf> (retrieved on 4 March 2024).

[32] Ibid., p. 6, 19-20.

[33] Federal Statistical Office, Omnibus 2021: Erhebung zur Internetnutzung, Steckbrief. *(Survey on the usage of Internet. Profile)* <https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/erhebungen/omn2021.assetdetail.22284438.html> (retrieved on 4 March 2024).

[34] See Federal Statistical Office, Allgemeine digitale Kompetenzen der Bevölkerung im internationalen Vergleich *(General digital skills of the population in international comparison),* 2021 <https://www.bfs.admin.ch/asset/de/22404704> (retrieved on 4 March 2024).

[35] Research Center for the Public Sphere and Society of the University of Zurich, Jahrbuch Qualität der Medien *(Yearbook Quality of the media),* 2022, <http://www.foeg.uzh.ch> (retrieved on 27 February 2024).

social networks; among 15- to 29-year-olds, 40% mainly via social media and 25% via online media.[36] Social media is rarely editorially moderated, and online media is usually less editorially moderated than traditional media. Many social media users can easily mistake false information for accurate information. Furthermore, certain affinities for conspiracy narratives and ideologies can contribute to users perceiving disinformation content that fits with already held beliefs as true and spreading it further.[37] Technological developments – namely AI – are also making it increasingly difficult to detect disinformation (see 2.2). Another study found that the practice of checking false information is relatively well established in society, particularly through checking the sender or consulting additional sources, including information from the state and authorities (68%), media websites (61%), but also Google (45%) and exchanges with relatives (43%).[38] Dedicated fact-checking websites are hardly established in the Swiss context.

When it comes to trust in the media, the Eurobarometer surveys give Switzerland slightly above-average values; for spring 2023, it was found that 53% of the population trusts the media (unchanged from 2021 and above the EU average of 36%).[39] Traditional media (72-82%) are trusted far more than internet sources (29%) and especially digital platforms (10%).[40] One study indicates that this trust is eroding to some extent, with general trust in the Swiss media falling from 50% in 2016 to 42% in 2023.[41]

4.4 Outlook

In the coming years, given international developments in power politics, it is very likely that certain state or state-commissioned actors will increasingly use influence activities and disinformation to try to destabilize Western societies, using the latest technological means. These activities will also target Switzerland. Switzerland is institutionally relatively robust against the threat due to its small size, regular democratic participation, high level of education and trust in political institutions and media. Nevertheless – as surveys on media and information literacy show – the changing use of media and technological developments are also increasing the challenges for Switzerland in dealing with influence activities and disinformation.

AI enables an even broader range of actors to create and spread sophisticated disinformation with less effort and at a lower threshold. As the algorithms underlying AI continue to be developed and perfected in the coming years, these should be even better tailored to their target audience and more credible, thus carrying an even greater impact. But AI also offers opportunities for regulation, fact-checking and uncovering influence activities and disinformation. These developments are strongly influenced by large technology companies that are introducing new technologies and pursuing their own self-regulation initiatives. Efforts to regulate large states or economic areas, such as the USA and the EU, are also likely to intensify and have an impact on Switzerland, offering Switzerland opportunities to adopt them or serving as a model.

[36] Reuters Institute Digital News Report 2023, co-published with Oxford University; Stefan Thommen et al., Medienmonitor Schweiz 2022, Untersuchung der Publicom, p.50-52, <https://www.medienmonitor-schweiz.ch/uploads/media/default/0001/02/MMS_2022_Jahresbericht.pdf> (retrieved on 27 February 2024).

[37] Research Center for the Public Sphere and Society of the University of Zurich, Falschinformationen, Alternativmedien und Verschwörungstheorien – Wie die Schweizer Bevölkerung mit Desinformation umgeht, *(False Information, Alternative Media, and Conspiracy Theories – How the Swiss Population Deals with Disinformation)* 2021, <https://www.foeg.uzh.ch/dam/jcr:96eb88c7-f0a2-4fc8-8fc2-6591e39195fa/Studie_01_2021.pdf> (retrieved on 27 February 2024).

[38] Vogler et al., Falschinformationen, Alternativmedien und Verschwörungstheorien (*False information, alternative media, and conspiracy theories*), p. 31.

[39] European Commission, Standard-Eurobarometer, Die öffentliche Meinung in der Europäischen Union *(Public Opinion in the European Union),* Mai/Juni 2023, p. 74, <https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=88065> (retrieved on 4 March 2024).

[40] European Commission, Standard-Eurobarometer, Die öffentliche Meinung in der Europäischen Union *(Public Opinion in the European Union),* January/February 2022, p. 46ff. <https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=81061> (retrieved on 4 March 2024).

[41] Nic Newman et al., Reuters Institute Digital News Report 2023, p. 103, <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf> (retrieved on 5 March 2024).

5. Legal Foundations in Switzerland

Various legal documents, notably those relating to political rights and the media, the Intelligence Service Act, the Criminal Code in general, as well as texts on security policy bodies and police duties, contain relevant provisions for dealing with influence activities.

The constitutional guarantee of political rights protects the free formation of will (cf. article 34 paragraph 2 of the Federal Constitution [SR 101]). Generally protected is the dissemination of false information by freedom of expression within the meaning of article 16 of the Federal Constitution and article 10 of the European Convention on Human Rights and, depending on the situation, freedom of the media within the meaning of article 17 of the Federal Constitution. In its jurisdiction, the Federal Tribunal assumes that individuals should be able to hear every opinion and information in order to be able to form their own opinion through the free exchange of all statements.[42] The robustness of the institutional information system is crucial to prevent and contain possible influence activities and disinformation. The Federal Council's information policy is based in particular on Article 180 of the Federal Constitution, Article 10 of the Government and Administrative Organisation Act (RVOG), Article 10a of the Federal Law on Political Rights and the guidelines of the Conference of Federal Information Services.

The *expression* of opinion may be restricted according to the general rules of Article 36 of the Federal Constitution (legal basis, public interest or protection of the fundamental rights of third parties and proportionality), for example where personal rights are violated in the form of slander or defamation. Legally supported restrictions on disinformation also exist where the protection of public safety and order is affected.[43] Certain actions in the information space can also be punishable as an attack on the constitutional order (Article 275 of the criminal code).

Special rules apply to particularly sensitive areas of opinion formation, such as information broadcasts on radio and television, where the so-called "objective accuracy requirement" (Article 4 paragraph 2 Federal Act on Radio and Television [SR 748.40]) applies to editorial broadcasts with information content. This requirement is violated if information content is manipulated in such a way that the audience can no longer form their own personal opinion. To do so, anyone can contact the radio and television ombudsman's office and, after their report, lodge a complaint with the independent complaints' authority for radio and television (Articles 91-98 Federal Act on Radio and Television). Supervision of advertising content is in turn the responsibility of the Federal Office of Communications. In general, radio and television broadcasts must not impair the internal or external security of the Confederation or the cantons and their constitutional order according to Article 4 paragraph 3 of the Federal Act on Radio and Television. This provision also applies to advertising; however, there are no specific applied cases to date.[44] Legal regulations specifically for intermediaries do not yet exist in Switzerland, but are being developed.

The provisions of the Intelligence Service Act are applicable to the responsibilities of the Federal Intelligence Service regarding influence activities. The Federal Intelligence Service can deal with influence activities abroad if they are relevant to the situation of Switzerland in terms of security policy. Within Switzerland, its work is more restricted and only permitted if there is a relevant connection to terrorism, prohibited intelligence activities, proliferation, attacks on critical infrastructure or violent extremism (Article 6 paragraph 1 Letter a Nos. 1-5 Intelligence Service Act). The Federal Intelligence Service is in

[42] See for example BGE *(Decisions by the Federal Tribunal)* 135 I 292, E. 4.1, p. 296. In its jurisdiction on Article 261*bis* criminal code, the Federal Tribunal also stated: "In public debates it is often impossible to distinguish from the outset between untrue, half-true and reasoned criticism." (BGE 131 IV 23, E. 3.1, p. 28); Schefer Markus, Kommunikationsgrundrechte *(Constitutional rights concerning communication),* in: Diggelmann Oliver et al. (Hrsg.), Verfassungsrecht der Schweiz *(Swiss consitutional law),* Band II, 2020, p. *1413-1452, Rz. 89; Raphaela Cueni, Falsche und irreführende Informationen im Verfassungsrecht der Schweiz (False and misleading information in Swiss constitutional law)*, ex/ante 1/2019, 3, p. 12.

[43] See BGer *(Federal Tribunal)* 1P.336/2005 (20 September 2005), E. 5.3; EGMR, Mouvement raëlien Suisse v. Switzerland (13 July 2012), 16354/06.

[44] In the framework of its supervision activity, the Federal Office of Communications could proceed against a programme organiser who disseminates disinformation in its advertisement and thus endangers the internal or external security of the Confederation or the cantons. The supervisory proceedings could in such a case only address the Swiss organisers, with the measures mentioned in Article 89 paragraph 1 of the Federal Act on Radio and Television. From what point on there would be an effective endangerment would have to be determined on the basis of the concrete circumstances; however, with regard to programme autonomy, such an endangerment could not be assumed lightly.

principle not allowed to process information about political activity and the exercise of freedom of opinion, assembly and association in Switzerland (Article 5 paragraph 5 Intelligence Service Act).

Depending on the nature of the activity, influence activities and disinformation can affect police duties and, depending on the offence, the cantons or the federal government can initiate criminal proceedings. Crimes and misdemeanours against public peace (Article 258 ff criminal code) can be relevant, in particular intimidation of the population (Article 258 criminal code). Fraudulent misuse of a data processing system (Article 147 criminal code) as well as discrimination and incitement to hatred (Article 261bis criminal code) can also be taken into account.

The Federal Police (fedpol) can preventively confiscate material that can be used for propaganda purposes and whose content specifically and seriously calls for violence against people or objects. If there is suspicion of a criminal act, the authority securing it will forward the material to the relevant criminal authority (Article 13e Federal Act on Measures for the Preservation of Internal Security). If propaganda inciting violence is spread via the Internet, the Federal Police can, after consulting the Federal Intelligence Service, order the deletion of the website in question from a Swiss server or recommend that the Swiss provider block a foreign website. If influence and disinformation activities are emanating from criminal organizations, the Federal Police can, based on the so-called ZentG[45], conduct preliminary police investigations on its own authority and coordinate intercantonal and international investigations. This can for example be relevant, as Russian state actors are proven to be utilising criminal organizations for their own purposes.

The Federal Police can impose entry bans and expulsions on foreign nationals if a person's influence activities endanger the internal or external security of Switzerland (Article 67 paragraph 4 and Article 68 Federal Act on Foreigners and Integration). Furthermore, the Federal Police takes protective measures if disinformation endangers federally protected personnel (e.g. Federal Councillors) and/or leads to an increased need for protection of federal buildings. In the case of the fake energy posters (see 4.2), the Federal Police opened an investigation into an attack on Swiss national emblems (Article 270 criminal code).

Other relevant offences subject to federal jurisdiction in this context are: attacks on the independence of the Confederation (Article 266 criminal code), foreign operations and endeavours directed against the security of Switzerland (Article 266bis criminal code), prohibited acts for a foreign state (Article 271 criminal code), prohibited intelligence activities (Article 272 ff. criminal code), offences against the will of the people (Article 279 ff. criminal code; Article 23 paragraph 1 letter h code of criminal procedure) and violence and threats against authorities and officials (Article 285 criminal code).

6. Responsibilities and Measures Taken in Switzerland

In the 2021 Report on Security Policy, the Federal Council stated that the risk of influence activities and disinformation against Switzerland was increasing. In fighting against them, the following measures should be mentioned: strengthening situation monitoring and early detection (6.1), strengthening the resilience of Switzerland and its population in terms of prevention (6.2), regulation and sanctions (6.3), communication and access to official information (6.4) and exchange between authorities and internal and external cooperation (6.5).

6.1 Situation Monitoring and Early Detection

There are currently no structures in Switzerland with the goal of comprehensively identifying systematic influence in the information space, determining its intention and authorship and, if necessary, responding to it.

The federal bodies charged with the coordination of security policy, namely the Security Core Group and the Security Committee of the Federal Council, chaired by the Department of Defence, Civil Protection and Sports, have the task of assessing the security policy situation and coordinating cross-departmental

[45] Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten; SR 360c. *(Federal act on the central criminal police authorities of the Confederation and joint centres for police and customs cooperation with other states).*

security policy affairs[46]. Aspects of this topic have been dealt with on several occasions. The Security Core Group can, based on its deliberations, submit proposals to the Security Committee.

Within Switzerland, the Federal Intelligence Service can collect, examine or process information on influence activities only to a very limited extent. The Federal Intelligence Service covers influence activities abroad that are significant for security policy and focuses on the direct, concrete or potential threat to Switzerland posed by the intensified rivalries between the great powers. The Federal Intelligence Service tracks the influence activities associated with hybrid conduct of conflict, particularly those of Russia and China. This includes actors and activities abroad that undermine the uninfluenced formation of political will in Switzerland or in its strategic environment, as well as actors and activities in Switzerland if there is a relevant connection to terrorism, illegal intelligence activities, proliferation, attacks on critical infrastructure or violent extremism.

Media monitoring is carried out generally and permanently by the departments, the federal offices and the Federal Chancellery. The Federal Department of Foreign Affair's *Presence Switzerland* monitors media reports on Switzerland abroad, and regularly evaluates them. The Federal Chancellery and the cantons are conducting risk assessments with regard to the use of electronic transmission of voting results in federal elections. These also include possible attacks through disinformation.

The Federal Office of Communications monitors compliance with the Federal Law on Radio and Television, specifically its implementing provisions and licences, and verifies that the Swiss Radio and Television Corporation and private broadcasters fulfil their journalistic service mandates, including through quantitative programme analyses research institutes periodically carry out. Most other departments, federal offices and the Federal Chancellery also carry out, to varying degrees, media monitoring on a topic- or office-specific basis.

Awareness of influence activities also includes the tracking of relevant technological developments. Armasuisse Science and Technology and the Cyber Defence Campus are working on various research projects on technological aspects related to influence activities and cyber defence, in collaboration with Swiss universities. For example, the threat potential posed by AI-generated image data was analysed in a research project with the University of Applied Sciences Northwestern Switzerland (FHNW). Data science research contributes significantly to the detection of influence bubbles and the plausibility of trends in social networks. It is currently being carried out by the Cyber Defence Campus but is partially restricted by the legal framework of armasuisse Science and Technology. Data from social media may, for example, not be anonymized in order to be used in research work.

Disinformation can influence members of the armed forces even before they start their service or while they are carrying out their duties. The armed forces therefore monitor the information space on a daily basis but especially during deployments and operations, to detect actions against members or basic services of the armed forces at an early stage. These findings are incorporated into a weekly situation briefing by the Operations Command. The Cyber Monitoring sector, a unit of the Armed Forces Cyber Command, analyses information from websites and social media. It carries out a preliminary evaluation of the relevant data and provides contributions to the detection of influence activities against Switzerland without Swiss involvement. If this information is relevant to the armed forces, this can be carried out for the benefit of the armed forces and the military intelligence service within the framework of the military law, or for the benefit of the Federal Intelligence Service at its request and on the basis of the Intelligence Service Act.

The federal administration is cooperating with third parties such as researchers to acquire a better picture of how Switzerland is affected. A report from the University of Zurich on disinformation in Switzerland (2021),[47] commissioned by the Federal Office of Communications, is the most comprehensive study

[46] According to directives of the Federal Council of 25 January 2023, based on Article 30 of the Federal Act on Measures for the Preservation of Internal Security. The Security Committee of the Federal Council includes currently the Heads of the Federal Department of Defence, Civil Protection and Sports, the Federal Department of Justice and Police, the Federal Department of Foreign Affairs, accompanied by their Secretary-Generals, the State Secretaries for Foreign Affairs and for Security Policy, the Directors of the Federal Intelligence Service and the Federal Police, and the Vice-Chancellor.

[47] Vogler et al., Falschinformationen, Alternativmedien und Verschwörungstheorien. *(False information, alternative media, and conspiracy theories).*

on disinformation to date. The Federal Office of Communications has compiled the existing literature on disinformation and has initiated scientific research on disinformation in Switzerland, focusing on disinformation content, reception behaviour, characteristics of the audience and governance approaches. Influence activities fall under this research, which is, however, broader in scope and does not focus specifically on disinformation by states.[48]

6.2 Resilience through Awareness, Education and Media Literacy

Resilience and prevention include raising awareness of the phenomenon, its manifestation, possible consequences and the impact on Switzerland. The target groups of such activities are federal staff (including representations abroad), cantonal authorities, the public, political actors (e.g. parties) and media professionals.

Specifically, participants from the federal government and the cantons exercised how to respond to influence activities and disinformation in the event of a crisis event as part of the large-scale security network exercise 2019, thus raising awareness of the issue. Within the overall scenario of a terrorist threat, it was simulated how political threats, propaganda and disinformation could be used to stoke uncertainty among the authorities and the population, including through cyberattacks on federal and cantonal information portals and through targeted manipulation of the media. Although this was done by a fictitious terrorist group, similar challenges are likely to arise if state actors act accordingly in the information space.

With a view to the national elections in 2019 and 2023, the Federal Chancellery invited parties, major platforms, the National Cyber Security Centre/Federal Office for Cyber Security and the Federal Data Protection Commissioner to a meeting on "campaigns in the digital space". The objectives were to raise awareness of the threat posed by influence activities and to discuss possible protective measures. In addition, in the run-up to the national elections, privileged access was arranged with Google, Meta and TikTok, providing for direct contacts in the event of any manipulation and ensuring that official information was prominently displayed on these platforms.

Quality media with high journalistic standards and an interested, critical audience, as is generally the case in Switzerland, help contain the impact of influence activities. In fulfilment of the postulate Christ 21.3781 "Launch a strategy for future-oriented media funding now", the Federal Council has set out in a report various financing options and models for media funding that can be implemented regardless of the channel. Regarding the promotion of journalistic training and further education, the Federal Office of Communications is currently working on the implementation of the parliamentary initiative Chassot 22.417 on funding measures for institutions that offer training and further education for editorial staff of electronic media. In addition, the Federal Office of Communications has adopted a national action plan for the safety of media professionals in 2023.[49] In particular, media professionals shall be better protected from threats, violence and attempts at intimidation, all of which are likely to be encouraged by influence activities.

A central element of resilience and prevention against influence activities and disinformation is education. Elements of this are applied at all levels of education for children, young people and adults. Older adults are much more difficult to reach through educational efforts. The compulsory school curricula, which is the responsibility of the cantons, provide for political and digital education.[50] The aim is to enable young people to inform themselves about and participate in political and social life. Concretely, the individual regional-linguistic curricula teach skills in terms of subject matter, judgement, conduct and methodology in order to critically and responsibly deal with media and information. The topic of critical handling of media and information is also being reinforced in the revised framework curricula for general

[48] For some insights from these studies, see 3.1 und 3.3.

[49] See <https://www.bakom.admin.ch/bakom/de/home/elektronische-medien/medienpolitik/nationaleraktionsplan.html#:~:text=Der%20Nationale%20Aktionsplan%20f%C3%BCr%20die,Medienschaffenden%20in%20der%20Schweiz%20dar>.

[50] Federal Department of Economic Affairs, Education and Research, Conference of the Cantonal Directors of Education: Chancen optimal nutzen. Erklärung 2023 zu den gemeinsamen bildungspolitischen Zielen für den Bildungsraum Schweiz, 26. October 2023, *(Make best use of opportunities. Declaration 2023 on the common aims of education policy in the education area Switzerland)* <https://www.sbfi.admin.ch/dam/sbfi/de/dokumente/2023/10/erklaerung-chancen-2023.pdf.download.pdf/erklaerung-chancen-2023_d.pdf> (retrieved on 5 March 2023).

education in basic vocational training and for the vocational baccalaureate. Those responsible for vocational training are also contributing to the promotion of digital skills.[51] According to a decision by the Federal Council and the Conference of Cantonal Directors of Education in 2018, all high school students across Switzerland have been required to take computer science classes since the 2022/2023 school year at the latest. At the university level, the federal government is expected to fund the future *Open Education & Digital Competencies* programme on a project-related basis from 2025 to 2028. The aim is to support teachers in developing a digital culture in the classroom with a focus on the quality of digital media and the skills of students to evaluate digital data and face the challenges of AI.

Media associations, such as the Swiss Media Association, are contributing to (digital) media literacy among young people through projects.[52] The portal ch.ch, the joint information platform of the federal government, cantons and municipalities on life in Switzerland, explains how the population can recognize and deal with disinformation. The Federal Social Insurance Office, meanwhile, runs the national Youth and Media platform to promote media literacy.

6.3 Regulation and Sanctions

In 2021, the Federal Office of Communications, in cooperation with the Federal Chancellery, published the report "Intermediaries and communication platforms: impact on public communication and approaches to governance", which highlights the positive and negative social potential of digital platforms and discusses existing regulatory approaches in Europe.[53] On April 5, 2023, the Federal Council commissioned the Federal Department of the Environment, Transport, Energy and Communications (Federal Office of Communications) to prepare a consultation draft on the regulation of communication platforms. This will also address the challenges arising from the lack of law enforcement against digital platforms. It is based on the EU's *Digital Services Act* and aims to make in particular very large platforms more accountable through due diligence and reporting obligations. However, regulation affects disinformation only where the content is illegal.
As for sanctions, Switzerland has not adopted the EU's sanctions of March 1, 2022 against RT and Sputnik – important Russian news portals abroad that are close to the state. Even though these channels are tools of targeted Russian propaganda and disinformation, the Federal Council believes that it is more effective to factually counter false and harmful statements rather than banning them. The reach of these media in Switzerland is considered to be low.

6.4 Communication

A distinction must be made between means of communication used to respond to influence activities and disinformation on the one hand, and communication used to regularly inform the population and political actors in the interests of prevention, on the other.

Influence activities can be politically undesirable even if they do not violate the law. The Federal Council and the federal administration can correct false or misleading information that is disseminated to the public *(debunking),* but they use this option only with caution. On the one hand, the dissemination of false information falls under the right to freedom of expression, provided that it does not constitute a criminal offense. With the illusory truth effect, whereby often repeated – even false – statements are considered to be truer; debunking can even increase the effect of disinformation. Mistrust and the belief in a "true core" of a disinformation could even be strengthened if corrections by the authorities are perceived as particularly aggressive and vehement. The social media guidelines of the Conference of Federal Information Services define criteria for responding to disinformation on new information platforms "if it spreads beyond the community from which it originates or beyond communities close to it or is harmful".

[51] according to the revised framework curricula for those responsible for vocational training.

[52] See the dossier "Medienkompetenz" ("media literacy) of the Publishers' Association of Swiss Media, <https://www.schweizer- medien.ch/medienkompetenz>.

[53] Federal Office of Communication, Intermediäre und Kommunikationsplattformen: Auswirkungen auf die öffentliche Kommunikation und Ansätze einer Governance, *(Impact on public communication and governance approaches),* 17. November 2021. <https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/elektronische_medien/Zahlen%20und%20Fakten/Studien/bericht-kommunikationsplattformen-und-intermediaere-2021.pdf.download.pdf/Bericht%20Kommunikationsplattformen%20und%20Intermedi%C3%A4re.pdf> (retrieved on 5 March 2024).

As such, the federal administration generally makes corrections only in these cases.[54] For example, the Federal Department of the Environment, Transport, Energy and Communications communicated on the circulation of the false energy poster (see 4.2).

In contrast to debunking, research results show the importance of awareness-raising measures and the strengthening of personal responsibility for prevention *(prebunking)*.[55] The Federal Council is not currently pursuing immediate prebunking, which would provide information about specific emerging influence activities and expose and/or invalidate them in advance, as this would prerequire a detailed overview of the situation.

However, the Federal Council generally pursues a direct, comprehensive, multilingual, transparent and continuous information policy, which renders influence attempts more difficult. Information about Federal Council affairs, the activities of the administration, and on votes and elections[56] is disseminated in several languages and via several channels, including regular media conferences at which members of the Federal Council appear in person. The Federal Council's information is increasingly supported by explanatory videos and infographics. The VoteInfo application, a direct information channel developed with the cantons and municipalities, provides the general public with information and results on federal and cantonal votes. The communication measures mentioned above are likely to increase the reach of the information to certain target groups but can only meet the challenge of influence activities to a limited extent.

The Federal Chancellery is currently designing an information app for the Federal Council's communication as a direct channel to the population. According to a study by the opinion research institute gfs.bern in 2022, 70% of respondents find such an information app interesting, while 75% find the approach useful. This channel would be independent of the large existing social media platforms and could be shielded from possible influence activities. It could also be used both during a crisis and in the event of influence activities that would require a response from the Federal Council (push notification).

Disinformation can have serious consequences during crises relevant to civil protection, such as power outages. It can undermine the ability of state institutions to respond effectively to the crisis. False information, for example about the causes of a power outage, can fuel mistrust, causing citizens to disregard the authorities' instructions, such as evacuation orders or safety notices. The Alertswiss app and website, which are used by the federal government and the cantons as tools for warning, alerting and informing the population to cope with disasters and emergency situations, play a key role in this context. Alertswiss can serve as a direct communication channel to inform the population about event-related emergency situations and to combat the spread of disinformation by providing accurate, timely and verifiable information. In order to optimise the effectiveness of Alertswiss in the context of disinformation, stakeholders (users at federal and cantonal levels) are increasingly being made aware of this benefit in training courses, in specialist bodies and via the existing information platforms.

With regard to communication, it should be noted that in the event of an armed conflict involving Switzerland, other measures would have to be considered than those applicable in a normal situation. The Swiss Armed Forces are therefore working on the deployment of resources in all operational spaces of, including the information space, in the event of a conflict, which is not discussed in detail in this report. As an instrument of security policy, in the event of an armed conflict, the armed forces must, within the framework of the federal government's strategic guidelines, be able to conduct military operations in the information space independently or in cooperation with the civilian authorities.

[54] Federal Chancellery, Leitlinien für die Kommunikation in den Sozialen Medien *(Guidelines for Communication in Social Media),* May 2021, Article 7, <https://www.newsd.admin.ch/newsd/message/attachments/67321.pdf> (retrieved on 5 March 2024).

[55] Jon Roozenbek et al., A Practical Guide to Prebunking Misinformation, 2022, <https://interventions.withgoogle.com/static/pdf/A_Practical_Guide_to_Prebunking_Misinformation.pdf> (retrieved on 5 March 2024).

[56] Within the framework of the legal requirements; for federal referendums, see in particular Article 10a and Article 11 paragraph 2 of the Federal Act on Political Rights (161.1; BPR) and for National Council elections, see Article 34 BPR.

6.5 Coordination and Exchange

Due to the complexity and breadth of the topic, a close exchange of information and coordination within the federal administration and between the federal administration, media, platforms, research, and with international partners and institutions is necessary.

There is currently no central coordination and comprehensive situation analysis as the responsibilities are distributed. In recent years, however, approaches have been pursued to promote coordination and exchange. In order to determine the impact and to promote coordination within the federal administration on this subject, the Security Core Group and the Federal Chancellery conducted a survey on the topic in the federal administration in January 2021 to obtain an overview of ongoing or planned work on influence activities and disinformation in the federal administration. To this end, the Security Core Group identified contact points for the early detection and treatment of influence activities. The survey revealed that almost all administrative units can be affected. Since August 2022, a network of contact persons in departments and offices for influence activities exists, and the Federal Department of Foreign Affairs has organized several workshops within the federal administration on the topic. Coordination and discussion platforms also exist between the federal administration and external stakeholders as well as multilaterally.

Switzerland also exchanges information with partner states and in multilateral forums on how to deal with influence activities and disinformation. It considers this exchange to be an important measure, as influence activities affect, due to their transversal effects, multiple states, and potential responses and situation reports can be strengthened through international cooperation and coordination. Since Switzerland is not a member of various organisations or institutions (NATO, EU, G7), its access to information is not necessarily given, but there have been various expert meetings with the EU. Closer cooperation in this area was also initiated with the United Kingdom in 2023 and an annual exchange is maintained.

At the European level, the Council of Europe's Steering Committee on Media and Information Society is developing measures and recommendations to combat misinformation. For example, a committee of experts chaired by Switzerland published guidelines on combating misinformation and disinformation while complying with human rights standards through fact-checking and recommendations for the design of online platforms.[57] In 2020, the *Freedom Online Coalition,* of which Switzerland is also a member, published a joint statement on disinformation. At the end of August 2023, it announced the establishment of a task force on the trustworthiness of online information. The Federal Office of Communications is participating in the work of the Digital Policy Lab of the *Institute for Strategic Dialogue,* which was initiated by Germany and offers an exchange platform with like-minded states on topics of disinformation, hate speech and platform regulation. In 2022, as part of intergovernmental activities of migration authorities, the State Secretariat for Migration participated in a 10-point toolbox to strengthen NATO and EU mechanisms to resist hybrid threats, which may include the instrumentalization of migration flows, including in the information space.

7. Further Measures and Options for Action

An effective fight against influence activities and disinformation requires a whole-of-society approach. Isolated measures by one authority or institution will not be sufficient in view of the coordinated approach and the use of considerable resources by foreign state actors and technological developments. Complete containment of the threat is not possible in a free society and in view of the spread of new technological means, nevertheless various measures already mentioned should to some extent be expanded and supplemented by others, especially for situation monitoring, early detection and coordination.

Situation Monitoring and Early Detection

In future, the Security Core Group will regularly discuss the issue of influence activities and disinformation, at least twice a year, and if necessary, refer it to the Security Committee and the Federal Council. The departments represented in the Security Core Group and the Security Committee – the Federal

[57] Council of Europe, Guidance Note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human-rights compliant manner, March 2024, <https://rm.coe.int/cdmsi-2023-015-msi-inf-guidance-note/1680add25e> (retrieved on 5 April 2024).

Department of Defence, Civil Protection and Sports with the Federal Intelligence Service and the State Secretariat for Security Policy; the Federal Department of Justice and Police with the Federal Office of Police; the Federal Department of Foreign Affairs with the State Secretariat – can submit any measures for decision to the Federal Council. It will also be examined how the future analysis and situation assessment concerning disinformation can be coordinated with the aim of identifying influence activities in the information space by state actors, determining their authors and their intentions, and identifying measures. The existing work and monitoring of all federal offices concerned shall be incorporated and can be supplemented to obtain a more comprehensive picture of the situation and share information. Furthermore, the potential for expanding and institutionalising international exchange and cooperation on situational awareness will be assessed, particularly regarding access to and participation in databases and analyses of the European External Action Service and the United Kingdom on the multilateral system. Possible measures will further also be examined, such as a central and public fact-checking portal, for example through the funding of an independent supervisory body or research institute.

Resilience Through Awareness-Raising, Education and Media literacy

The topic for the comprehensive Integrated Exercise 2025, which the Federal Chancellery is organizing together with the Federal Department of Defence, Civil Protection and Sports and the cantons, will be a hybrid threat against Switzerland. In this exercise context, influence activities and disinformation, and how to deal with them, will play a central and key role. In addition, as part of the research assistance that the Federal Office of Communication has launched, a focus will be placed on the effect of disinformation in the short, medium and long term as part of a new programme to investigate disinformation in the context of opinion formation. A better understanding of the effects of disinformation in the Swiss context will help to assess the situation and support efforts of awareness-raising and prevention.

For all three language regions, the compulsory school curricula as well as the framework curricula of the upper secondary level include political and digital education. Various platforms of government agencies provide information about disinformation and offer courses on media literacy and political competence. Given the already very extensive range of courses, an expansion or deepening is not necessary in the short term. Thanks to the high level of flexibility and close cooperation between educational actors, there are rapid action options if necessary.

Regulation and Sanctions

The Federal Office of Communications is currently preparing a consultation draft on the regulation of very large communication platforms. As for potential new sanctions of the European Union against news portals that spread disinformation, the Federal Council will assess them, taking into account the concrete circumstances, proportionality and the benefits for foreign and security policy.

Communication

In light of freedom of expression, the Federal Council and the federal administration are cautious in correcting disinformation and a corresponding guideline exists from the Conference of Federal Information Services.[58] This principle will be upheld. The Federal Council will continue to communicate directly, comprehensively and transparently through various channels, which renders influencing activities more difficult. The additional work and exchange within the framework of analysis and situation reports should be incorporated into the federal government's deliberations regarding the communication of incidents and potential diplomatic measures.

Exchange and Coordination

Since 2022, the federal administration has maintained a network of contact persons for influence activities, and regular workshops on the topic are organized within the administration. This exchange serves to promote a common understanding of this security threat, relevant developments, the situation and the relevant activities at the federal level, and to derive and coordinate measures. Furthermore, experts from academia or abroad as well as persons responsible for this subject in other countries are part of this

[58] Federal Chancellery, Leitlinien für die Kommunikation in den Sozialen Medien *(Guidelines for the Communication in Social Media),* May 2021, Article 7, <https://www.newsd.admin.ch/newsd/message/attachments/67321.pdf> (retrieved on 5. March 2024).

exchange. The ongoing international exchanges with partner states and in multilateral forums to exchange specialised knowledge and to strengthen the situation awareness are continuously maintained and are to be expanded where appropriate. Exchanges within the federal administration are to be expanded in the future and, if necessary, institutionalized. In this context, links to work on transnational repression must also be examined. The threat posed by influence activities and disinformation and their significance for security policy have increased, which in turn increases the need for coordination. Coordination with the federal bodies dealing with security policy is to be strengthened and the, in the future, more closely coordinated analysis and assessment of the situation should be incorporated into their deliberations as well as exchanges within the federal administration.

8. Glossary

Disinformation: Misleading or completely fabricated information that is deliberately used to influence public opinion and political processes, attack the credibility of institutions and the media, or sow doubts about the reliability of information (see 2.1).

Fake news: False allegations of fact made in bad faith and spread for the purposes of political manipulation, financial or other personal gain, deriving power from the new dynamics of social networks.[59]

FIMI: The EU uses the term *Foreign Information Manipulation and Interference.* For the EU, FIMI corresponds to non-illegal behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. The EU has developed a standardized analysis framework for this.

Influence activities: Influence activities in the information space encompass a wide range of tools, including disinformation, and aim to manipulate the perception, thinking and actions of individuals, groups and societies. These activities can be carried out by state or non-state actors (see 2.1).

Influence operation: An influence actor can coordinate several activities in the information space as parts of an influence operation.

Influence campaign: In an influence campaign, an influence actor who has a high degree of skills and resources coordinates influence operations. The individual activities underlying the campaign can be based on various means of influence (e.g. disinformation, cyberattacks or through exercising pressure).

Malinformation: True information spread with the intent to cause harm, often through leaks of information not intended for the public.

Misinformation: Misinformation can also simply describe information that is factually incorrect, erroneous or misleading, regardless of its use and the actor's awareness that the information is false.

Propaganda: As a tool for influencing opinions, propaganda can be essentially truthful; however, the information is deliberately chosen, coloured and interpreted in such a way that it creates and promotes a certain opinion or viewpoint in the recipient. When diplomatic channels considered legitimate, such as the X/Twitter account of a foreign mission, spread disinformation, these categories merge. Propaganda is an element of influence activities in the information space and differs (partially) from disinformation in that it can also be true. Propaganda is often based on proven facts, but these are supplemented by deliberately manipulated, one-sidedly contextualized or decontextualized interpretations.

[59] Report oft he Federal Council, Rechtliche Basis für Social Media: Erneute Standortbestimmung. Nachfolgebericht des Bundesrates zum Postulatsbericht Amherd 11.3912 „Rechtliche Basis für Social Media“ *(Legal basis for social media: new assessment. Follow-up report of the Federal Council to the postulate report Amherd 11.3912 "Legal basis for social media"),* May 2017, <https://www.bakom.admin.ch/dam/bakom/de/dokumente/informationsgesellschaft/social_media/social%20media%20bericht.pdf.download.pdf/social-media-bericht-2017-DE.pdf> (retrieved on 5 March 2024).