Support to Strategic Foresight

Non-state Actors and the Information Environment 2050 - Four future scenarios

Lisa Bergsten, Sofia Olsson

In 2024, the Swedish Defence Research Agency conducted a study on what the digital information environment might look like in 2050 and the role that non-state actors could play in it. The study was carried out on behalf of the Swedish Armed Forces. This summary presents the four scenarios and the game-changers that were identified and constitute the results of the report. The full report includes a description of the methods used, an overview of what the information environment in 2050 could look like, and conclusions about the consequences for the Swedish Armed Forces' operation environment.[1] The four scenarios should be viewed as *possible* futures. They represent a Swedish perspective, with Sweden serving as the setting for each scenario. They may be considered somewhat extreme, unlikely, or even threatening. This is intentional. One of their purposes is to expand the reader's perspective and create a basis for discussion about what to expect in the future. The four scenarios operate across two levels, each with its own spectrum: one level for governmental regulation, ranging from high to low, and one for conflict, ranging from peace to war. The four scenarios are *DigiSvea — The Innovation Hub*, *Cracks in the Barricade*, *Polarising Digital Anarchy*, and *A Digital Front*. Figure 1

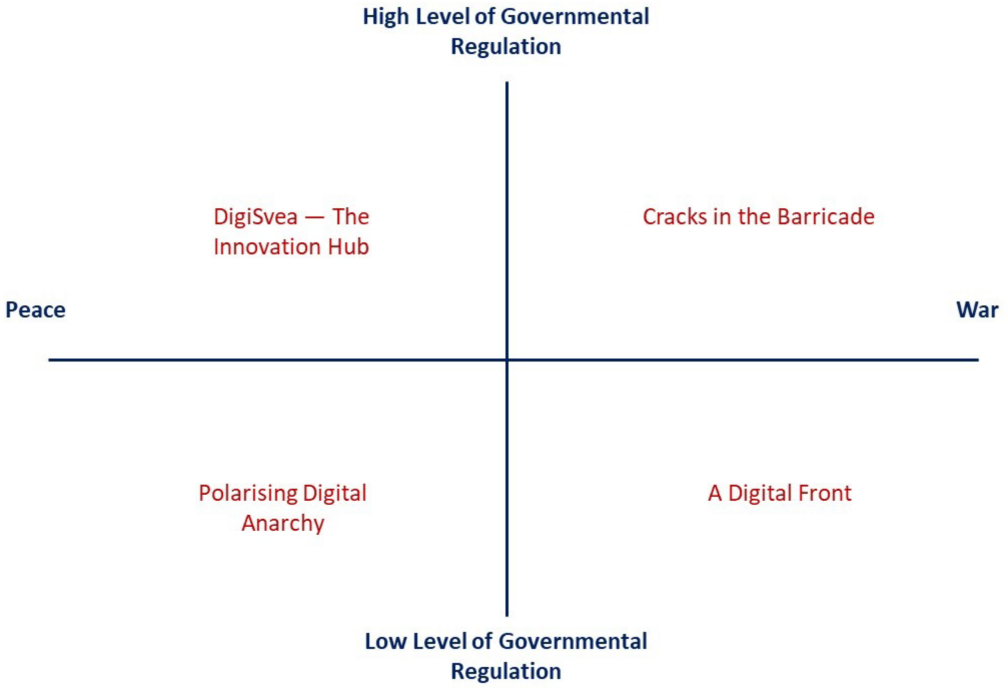
High Level of Governmental Regulation
DigiSvea — The Innovation Hub
Cracks in the Barricade
Peace
War
Polarising Digital Anarchy
A Digital Front
Low Level of Governmental Regulation

Figure 1. Illustration of the scenarios and the two spectrums on two levels: the level of governmental regulation and of war or peace.

[1] L. Bergsten and S. Olsson. *Framtidens informationsmiljö och icke-statliga aktörer.* FOI Memo 8569. Stockholm: The Swedish Defence Research Agency, 2024.

FOI Memo 8610
Project no: E139121
Approved by: Karolina Gasinska Singh

November 2024

presents a visual illustration of these scenarios and their placement along both spectrums and levels.

This summary presents each scenario individually and is followed by a section describing the game-changers identified. The game-changers are not included in the scenarios but are critical uncertainties, events, processes, and factors that drastically and significantly alter conditions, thereby reshaping future developments. These game-changers can disrupt these four scenarios in different ways and thus generate alternative pathways forward. A short overview (Table 2) where the four scenarios are compared and contrasted, concludes this summary.

Scenario 1: DigiSvea — The Innovation Hub

- High level of governmental regulation
- Peacetime
- Sweden is a leader in innovation and technology development
- The state's super-app, DigiSvea, requires users to complete ID verification
- Peaceful as well as violent actors organise themselves offline

Sweden is in a strong economic position in 2050. Rare earth metals and other deposits, combined with a successful green transition, have paved the way for prosperity. The tradition of engineering and the widespread digitisation of society that began in the 21st century have borne fruit; Swedish companies that offer digital services and tools based on large AI models, which require enormous amounts of energy to maintain and uphold, such as advanced AI assistants, wearable technology, and automated household services, are successful both nationally and internationally.

The tone of social media was harsh in previous decades, with polarisation and radicalisation fuelled by anonymous accounts and fake profiles. The mental health of children and youths was deteriorating, and the general population's physical well-being suffered. The regulations imposed on the big social media giants was not considered good enough to curb the negative development. Although screen-time restrictions for children and youths were proposed in the 2020s, a law was not adopted until 2040, and now applies to adults as well.

Around the same time, ID verification on the primary platforms of the digital information environment was introduced. Several large social media companies did not accept this. They left the country, prompting the rise of the state-owned super-app, *DigiSvea.*

Sweden simultaneously banned platforms perceived to be particularly harmful to children or to be covert influence operations from a foreign power. Slowly, the population's mental as well as physical health improved. Now, due to the more controlled information environment, people are more involved in civil society, which in 2050 is flourishing.

The majority of citizens rely on *DigiSvea* as their primary source of communication. The app consolidates various digital services, acting as a platform for everything from social media and communication to payments and official government services. Gradually, the population accepts *DigiSvea* as a part of daily life, seeing it as a trade-off between restrictions of privacy and personal integrity for enhanced safety and security. It is no longer possible to remain anonymous, since ID verification is necessary for the creation and use of an account in *DigiSvea*. There are some platforms that remain unrestricted, despite the state's high level of control over the digital information environment. These are "homemade", created from open-source code that the previously dominating social media giants were forced to release in the 2030s during a major regulatory wave within the European Union. Antagonistic actors find it difficult to conduct large-scale information-influence campaigns via these digital communication platforms, but local campaigns do occur.

Virtual games also remain unregulated, although screen-time restrictions apply. The games create largely unlimited worlds. For some users, they coincide with reality through virtual, augmented, or extended reality technologies.

These uncontrolled platforms and games become meeting places for individuals and non-state actors who, for various reasons, want to operate beyond the state's control. This includes groups who argue that the price of security is too high. Concerns about the long-term effects of the major limitations on freedom of expression that the regulation of the information environment entails simmer beneath the surface. The uncontrolled platforms are not well known, and their usage is geographically limited, which makes recruitment to and mobilisation of different social movements challenging. To gain attention and traction, more and more people are taking to the streets and demonstrating. Many of them are peaceful, but some groups use violence and commit sabotage. The communication within these groups occurs primarily outside of the digital information environment and often beyond urban centres, where sensors and cameras make it difficult to escape surveillance.

Scenario 2: Cracks in the Barricade

- High level of governmental regulation
- War in Sweden's immediate area; Sweden is in a state of heightened alert
- Geographically limited information environment
- Decreasing acceptance of regulations
- Significant foreign and domestic malign influence campaigns against specific groups

Sweden is involved in a war in its immediate area, not only through its NATO membership but also because of strong historical bilateral relations with the invaded country. The country has been in a state of heightened alert since the conflict began. The government implemented emergency measures, significantly restricting personal freedoms such as privacy and free speech.

Sweden has consequently enacted strict regulations over its digital space. Surveillance of the digital information environment has intensified, and laws protecting data and individual rights have been suspended or limited, or put "on pause," all aimed at shielding Sweden from foreign malign influence and hostile actors. To be active on the major platforms, ID verification is required.

The government has established a "digital barricade" to control access to information. Within Sweden's borders, only certain websites can be accessed as the government tries to prevent external manipulation and influence attempts. AI systems monitor the digital environment, scanning for disinformation and cyber threats. Official state channels dominate the media, promoting unity, support for the war, and resistance to foreign influence. They aim to maintain and strengthen the population's will to defend and societal resilience.

The state has also introduced a series of regulations that gives it access to data owned by private companies. Several large data servers are located in Sweden; by seizing control of these servers and sharing specific data with its allies, Sweden seeks to assist them. Many companies comply with the new rules and voluntarily relinquish the data, while others refuse. This also applies to other sectors of society. For example, certain infrastructure has been incorporated into the common cyber defence.

Since the invasion began, there has been an understanding amongst the Swedish population that restrictions on free speech are necessary. However, as time goes by, acceptance gradually decreases. More people seek information beyond the state-controlled channels.

Using a mix of new and old technologies, residents access information outside the geographically limited information environment. Through these cracks in the barricade, domestic and foreign actors try to influence the Swedish population, and targeted disinformation campaigns circulate. Narratives that exploit Sweden's historical sensitivities and national pride portray the government as increasingly authoritarian and oppressive. One recurring narrative focusses on the idea that the Swedish state, through its control of the digital space, is suppressing free speech and stifling dissent. Another effort tries to undermine the Swedish military's role in the conflict by circulating manipulated videos online that falsely depict Swedish soldiers committing human rights abuses against civilians. These fabricated videos are designed to erode the public's trust in the military and weaken its support for Sweden's involvement in the war.

Segments of the Swedish population begin to align with these opposing narratives. Protests against Sweden's involvement in the war are more frequent, both within Sweden and among its allies. However, there is also an overwhelming solidarity with the invaded country, leading to counter protests by those who believe in supporting the war effort. The invader, whose state church plays a political role, uses religion to sway public opinion. Some religious communities in Sweden amplify the invader's propaganda, framing the war as a just cause. This resonates with parts of the population who are searching for meaning amidst the chaos, and are trying to make sense of an increasingly hostile world.

Scenario 3: Polarising Digital Anarchy

- Low level of governmental regulation
- Peacetime
- Backlash against earlier restrictive regulation
- Sanctuary for antagonistic non-state actors; strained diplomatic relations

Many search the information environment for answers to big questions. Sweden has transformed into a hub for non-state actors operating in an almost completely deregulated digital space. After several years of heavy government oversight and restrictions on personal integrity and freedom of speech, a backlash led to the dismantling of many regulations and laws, heralded as a victory for Swedish democracy. The country's information environment has become a haven for non-state actors owing to the state's fragmented control over the digital space. Criminal organisations, extremist groups, and digital activists take advantage of the lax oversight to carry out activities that range from propaganda and recruitment to the remote tactical guidance of groups who conduct attacks in other European countries. The mobilisation includes people who are physically within and outside of Sweden. Violent extremist groups in particular thrive in this unregulated environment, using Sweden as a base for training and mobilising members across the continents. At the same time, Sweden also becomes a sanctuary for global human rights activists and political dissidents, who utilise the freedom of the digital space to organise and spread their messages.

At the same time, the digital information environment has transformed daily life. The AI revolution has allowed many Swedes to work fewer hours, spending more time in augmented and virtual reality, especially for entertainment. As political tension and climate change make the outside world feel uncertain, many seek distraction in the digital space. However, a growing number of people choose to step away from that realm in favour of in-person interactions.

This shift highlights social inequality, as wealthier individuals can more easily disconnect and outsource their digital presence, making face-to-face meetings a status symbol that businesses have begun to cater to.

Diplomatic relations with other nations, particularly within the European Union, become increasingly strained. However, the EU has little regulatory power to oppose this development; national law has taken precedence after nationalist forces dominated the Union for several years. This once-strong institution has lost influence, and cooperation now only occurs on basic issues such as economics and trade.

This digital fragmentation not only affects Sweden's foreign relations but also has profound effects on its social fabric. The lack of centralised control allows disinformation to flourish, creating a chaotic information landscape where it is difficult to discern truth from fiction. Extremist groups, fuelled by this chaos, find new recruits among those disillusioned with the government and mainstream society. Radical environmental movements, in particular, gain momentum, with young women and girls becoming especially involved in violent all-female climate movements. Anyone can create their own platform, their own content, and broadcast it directly through their choice of technology. Many of these platforms are community-centred or locally rooted for individual schools, companies, organisations, and associations. The digital information environment has returned to the "early days" of the internet, with more niche platforms complementing the big giants, who are still active in Sweden but not very popular. The freedom to create community-centred platforms and niche communities has allowed individuals to operate within completely isolated "filter bubbles." These bubbles reinforce existing beliefs, often unchallenged, which in some cases lead to radicalisation and a deeper polarisation of Swedish society.

Scenario 4: A Digital Front

- Low level of government regulation
- War on Swedish territory
- Strong will to defend and high societal resilience
- Volunteer Information and Cyber Army
- Vulnerable digital information environment

By 2050, Sweden is embroiled in a war that extends far beyond the physical battlefield, with the digital space playing a crucial role in the conflict. The war is fought not only on the traditional battlefields but also within the information and cyber environments, where cyberattacks and disinformation campaigns constantly reoccur. Central to Sweden's defence strategy is a volunteer-based "Information and Cyber Army," composed of private citizens, corporations, organisations, and defence associations that support the armed forces and the state. These groups collaborate with the military and government agencies to protect Sweden's digital infrastructure and combat cyber threats and are part of Sweden's total defence. A number of companies have restructured their operations to support Sweden's population, particularly its state authorities and Armed Forces. The war has stimulated innovation, and many areas are developing quickly due to relaxed regulations. The state enjoys a high level of trust among citizens, and there is a strong spirit of resilience.

Over the decades, coding and cybersecurity have become essential parts of the school curriculum, ensuring that most Swedes possess the skills necessary to contribute to national defence in the digital space. This widespread competence allows the population to handle digital threats effectively, particularly as key AI-driven services falter due to attacks on infrastructure. Citizens, companies, and defence associations jointly develop capabilities, such as drones. Protecting society's critical infrastructure and secure communications for citizens are top priorities that unite the Swedish population. The war has a strong and constant presence in everyday life, and dominates the information environment. Technological advancements have brought the battlefield closer than ever, with real-time updates and visuals from the frontlines delivered directly to the public. To maintain high morale and resilience, the government has made significant investments in sports, culture, and entertainment, with both public service and private entities playing their part.

The Information and Cyber Army works closely with both the state and the editorial media to inform the public about the progress of the war. Most of the time, people follow the government's official narrative, but other perspectives and counternarratives are circulating. Disinformation and misleading content are disseminated relatively freely in the digital information environment. False information comes from all different directions, including from countries that Sweden has perceived as allies or neutral. International digital grassroots movements work to counter disinformation and attempt to trace its origin. While it remains difficult to determine the actual senders, it appears that antagonistic movements inside and outside Sweden are trying to influence the public's will to defend and societal resilience, as well as to undermine trust in state institutions.

Cybercriminals not only use this chaotic information environment to commit crimes, but they also act as proxies for foreign powers. Other non-state actors, including terrorist organisations, take the present opportunity to recruit members. Although critical thinking and source criticism are generally high within the Swedish population, which has spent decades navigating an information environment full of misleading content, a minority remains receptive to it, particularly segments of the population who feel that their situation has become significantly worse since the war began. Despite the chaotic situation, Sweden's voluntary Information and Cyber Army stands as a testament to the strength of civil society. The ability of ordinary citizens to defend their country in the digital realm has become a critical component of Sweden's Total Defence, blurring the lines between strictly military and civilian roles.

Game-changers

Table 1 lists the game-changers identified. A game-changer is a critical uncertainty, an event, process, or factor that drastically and significantly alters conditions, thereby reshaping future developments. These game-changers can disrupt these four scenarios in different ways and thus generate alternative pathways forward. ■

Table 1. Game-changers.

Game-changer	Description
The Unknown Technological Revolution	The next technological revolution emerges from a development that cannot be predicted today, possibly due to dual-use technology or a combination of technologies. The implications for the information environment are unforeseeable.
Dictatorship in Sweden	Sweden becomes a dictatorship, with restricted freedoms and repression. The heavy control and monitoring of the information environment limits the operational space for non-governmental actors and individuals.
A Return to an Analogue Way of Life	A large portion of society rejects digital platforms, opting instead for more "analogue" communication. The digital environment may become a space primarily for services rather than communication.
General AI	If General AI evolves from theory to practice, the consequences would have transformative but difficult-to-assess impacts on society and the information environment. Theoretically, General AI would not just replicate human actions, but holistically understand context and the application of those actions.
Mass Destruction of Data	An event occurs that leads to the complete destruction of data. As a result, parts of or all of society could revert to a pre-digital state for an extended period of time.
Rationing of Energy and Electricity	Limited access to electricity and energy forces society to prioritise resources. This could involve the introduction of "ration cards" to save energy, as well as affecting the digital information environment and the services provided through it.

Overview of the Scenarios

During the study, two more factors than war/peace and the level of governmental regulation were identified as critical for the future development of the information environment and non-state actors: platforms and the time that individuals spend in the digital information environment. Therefore, Table 2 provides an overview where these critical factors as well as both antagonistic and non-antagonistic non-state actors are included. This is to contrast and compare the scenarios through each factor and provide an easy overview of the scenarios.

Table 2. An overview of the four different scenarios.

Scenario	DigiSvea — The Innovation Hub	Cracks in the Barricade	Polarising Digital Anarchy	A Digital Front
War/Peace	Peace.	War on the territory of an allied state. Sweden is involved militarily.	Peace.	War on Swedish territory.
Level of Governmental Regulation	High.	High.	Low.	Low.
Platforms	The super-app, DigiSvea, dominates. Small niche and locally rooted platforms exist.	The information environment is geographically limited, but it is possible to reach platforms outside of the government's digital control.	Niche platforms complement the global giants. Many are locally rooted.	Unspecified.
Antagonistic Non-state Actors	Organise and communicate outside of the digital information environment. Use sabotage and violence. Limited opportunities to conduct large-scale influence campaigns, but local ones occur.	Conduct influence attempts on platforms beyond governmental control. Target specific groups deemed as vulnerable.	Involved in digital mobilisation, organisation and training of the like-minded in and outside of Sweden. Conduct remote tactical guidance of acts of violence in other countries takes place.	Cybercriminals are active, and used as proxies by foreign powers. Groups recruit for their own cause and/or spread dis- and misinformation.
Non-antagonistic Non-state Actors	Companies are successful in providing digital services. Civil society is flourishing. Peaceful demonstrations occur.	Some companies cooperate with the state but generally have a low level of agency. Protests against Sweden's involvement in the war occur, as do demonstrations in support of the invaded country.	Mobilise and organise supporters as well as influence global opinions from Sweden. Are involved in physical associations. Create their own platforms and content.	Participate in the voluntary Information and Cyber Army. Participate in multinational digital movements. Companies support the Swedish state in various ways.
Time Spent in the Digital Information Environment	Legislation regulates the population's time in the information environment through screen-time restrictions.	Unspecified.	People spend a lot of time in the information environment, e.g., for entertainment. Digital presence is required for several community services; those who can afford it outsource it.	Unspecified.

Lisa Bergsten *is an analyst specialising in futures studies, while* ***Sofia Olsson*** *is an analyst focussing on the information environment and strategic communication. Both are active in the Division of Defence Analysis at the Swedish Defence Research Agency.*

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Tel: +46 8 5550 3000
www.foi.se