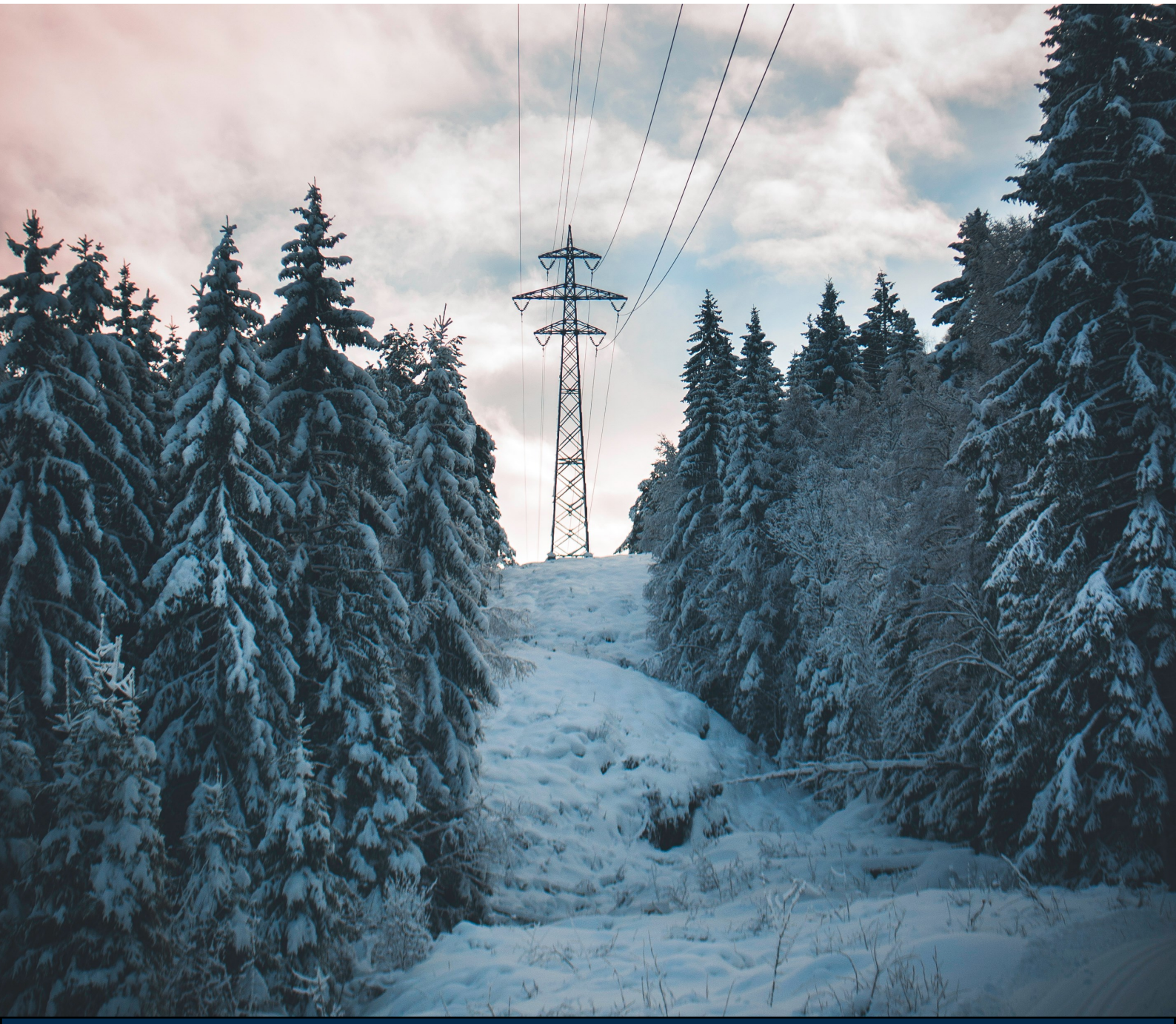
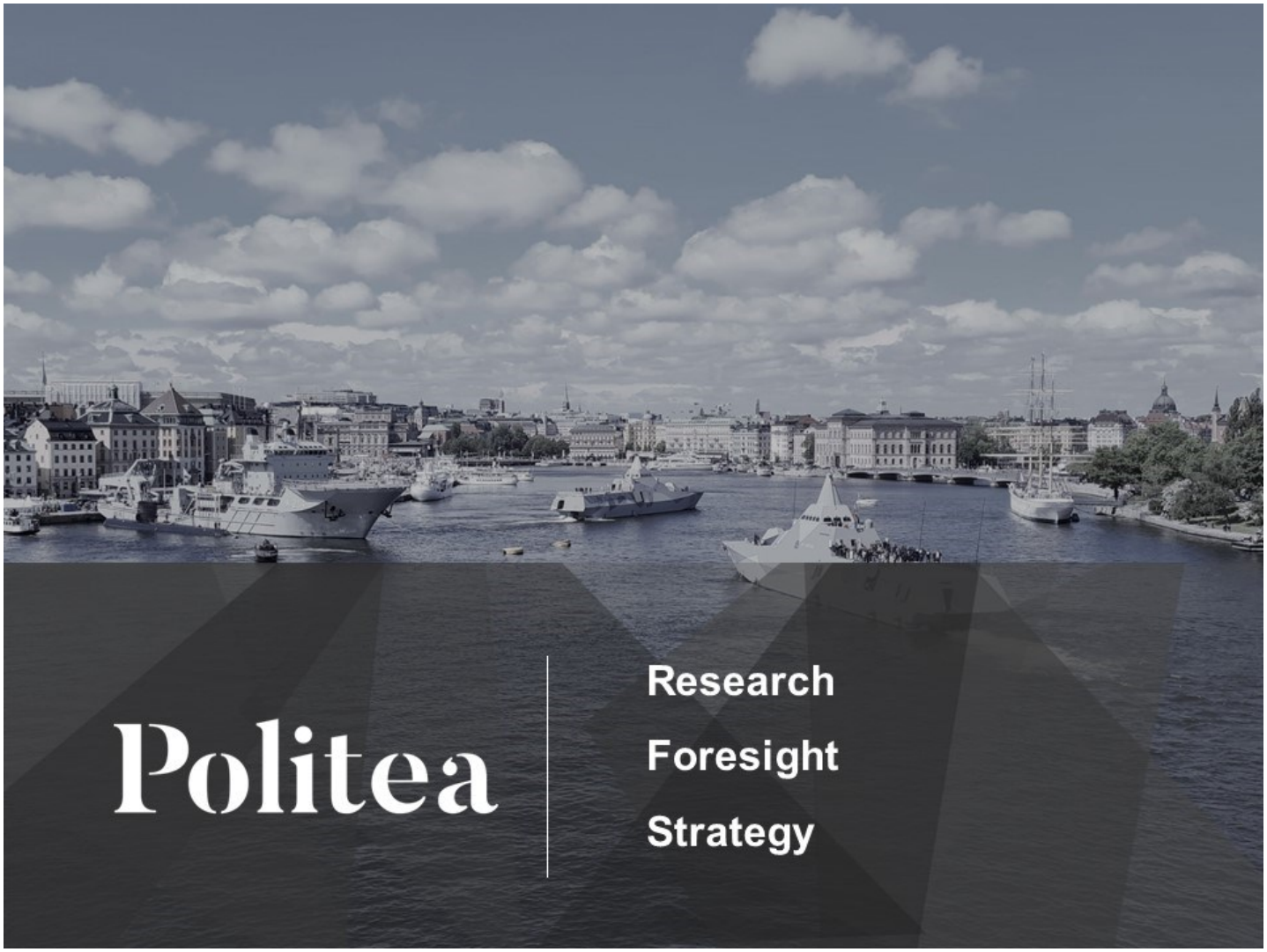
Sweden and hybrid threats

Legal frameworks, actors and societal resilience



Politea



About Politea

Politea is an analysis company focusing on international political risk, geoeconomics, and technology, based in Stockholm, Sweden. With research, foresight, and strategy development, Politea helps companies and authorities to navigate in an increasingly turbulent environment and position themselves for the future.

About the report

This is a public version of a report commissioned by The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). The Hybrid CoE has the full right to draw on any analysis of the report for their comparative work in the field.

Authors:

Dr Björn Fägersten. CEO Politea

Jens Holzapfel. Security and intelligence professional with 20 years of experience from Sweden's defence and national security community.

Published in October 2023

Sweden and hybrid threats

Legal frameworks, actors, and societal resilience

A background report by Björn Fägersten and Jens Holzapfel

Introduction

This report explores Sweden's strategies in countering complex hybrid threats, which combine conventional and unconventional tactics like cyber-attacks and misinformation. We have conducted interviews with several current and former senior officials and agency levels in the Swedish hybrid threat community and analyzed laws and unclassified information in relation to the coordination of countering hybrid threats. In conclusion, Sweden lacks specific legislation, a robust policy coordination structure, and a designated responsible agency or department for addressing hybrid threats. Given the ever evolving and unconventional nature of hybrid threats, the responsibility is dispersed among multiple actors, and incidents are managed within the framework of regular agency and departmental activities. However, within the scope of this report, three areas have been identified where, at least partially, specific structures have emerged in response to the challenge:

1) Establishment of a national cybersecurity center to address antagonistic cyber threats.
2) Creation of a dedicated agency for psychological defense.
3) Legislation aimed at countering foreign acquisitions and investments in sensitive technology.

The report starts by examining Sweden's legislative frameworks and reforms aimed at enhancing resilience against these threats, highlighting the importance of policy coordination, interagency cooperation, and efficient information sharing. The discussion then shifts to assessing and prioritizing hybrid threats, evaluating the effectiveness of Sweden's responses, and the challenges faced.

An integral part of the analysis is the role of the private sector and the impact of Sweden's membership in the EU and NATO, underscoring how international cooperation bolsters its defense strategy. Concluding with lessons learned from Sweden’s experiences, the report offers

insights into the evolving strategies in national and international security, emphasizing a holistic approach to managing hybrid threats.

Key legislative frameworks and legal reforms

The overarching legal framework for addressing hybrid threats in Sweden is rooted in the country's peacetime crisis preparedness system. Under this system, independent agencies, separate from the political sphere, are tasked with handling specific issues within their respective areas of responsibility. They are expected to operate within their legal mandates and as closely as possible to the affected level. In addition, these agencies are obligated to collaborate with one another within their areas of operation. Furthermore, the principle holds that the agency responsible for a particular issue during peacetime retains that responsibility during heightened preparedness, including situations involving hybrid threats. Thus, from a legal perspective, hybrid threats refer to activities preceding war.

The Swedish government, independent of the requirement for parliamentary approval, has the authority to declare that Sweden is at war. In such cases, special laws related to activities such as military service and disposals are in effect. During periods between war and peacetime, the government can declare a state of heightened preparedness. In October 2022, a reform of the preparedness system was implemented, which regulates the crisis preparedness of agencies during both peacetime and heightened preparedness. The primary distinction between peacetime and heightened preparedness that during the latter, agencies are expected to prioritize their efforts toward supporting total defense.

A significant aspect of this framework is the differentiation between internal and external security responsibilities. The Police Authority (Polismyndigheten) and the Security Service (Säkerhetpolisen) are responsible for internal security, while the Armed Forces oversee external security. This means that many instances of hybrid threat to that may occur during peacetime and heightened preparedness must be investigated or handled as criminal matters by the police. If the offense in question pertains to national security, it falls under the jurisdiction of the Security Service. This also applies to cyberattacks during peacetime, which are legally considered cybercrimes and are thus investigated by the police or by the Security Service if they relate to national security. While the Armed Forces can provide limited support to the Police Authority and the Security Police even during peacetime, such support is limited to counterterrorism efforts and logistical assistance, such as helicopter resources. At the time of this writing, a political debate on providing the police with additional authority to draw on military resources is ongoing in response to significant gang-related incidents.

To uphold external security and protect Sweden's territory, the Armed Forces have legal support for peacetime in cases involving, for example, violative aircraft or maritime vessels. Such interventions by other states often serve as a demonstration of strength, which in itself can be seen as an expression of a hybrid threat. It is worth noting that the regulations governing the Armed Forces peacetime protective duties do not explicitly account for hybrid scenarios such as cyberattacks or other forms of hybrid threats.

Legal Framework for Psychological Defense

Disinformation, information influence, and influence operations are activities that are often associated with the concept of hybrid threats in Swedish security policy discourse. To address these issues, the Swedish Psychological Defence Agency (MPF) was established on January 1, 2022. The agency's mission is to coordinate the efforts of other actors in the field of psychological defense, identify, analyze, and provide support in countering disinformation influence, as well as enhance the population's ability to resist influence campaigns and disinformation.

In brief, the Swedish constitution, in the form of the Instrument of Government, the Freedom of the Press Act, and the Freedom of Expression Act, protects individuals' rights to express themselves, even if the information is false, constitutes disinformation, or involves unauthorized information influence, regardless of the sender. In the preparatory work leading up to the establishment of MPF, it was not specified in detail what countering information influence entails. However, it was established that countermeasures must be lawful, uphold freedom of expression, be factual and impartial, respect freedom of opinion, and not engage in opinion shaping. In practice, providing accurate information is the only tool considered appropriate during peacetime. Authorities may also inform the public about the influence of information. In times of war, however, or imminent war, the agency is to support the government and propose measures that reduce the attacker's ability and intention to engage in aggression.

Only publications that violate the law and, therefore, fall outside the scope of freedom of expression and information laws (e.g., publications that breach national security, constitute defamation, or involve unlawful threats) can be countered with means other than accurate information, typically through criminal investigations by competent authorities. Regarding criminal statements, specifically in social media, responsible entities are obligated to remove them upon detection. These countermeasures are reactive, and authorities are not allowed to engage in censorship or otherwise proactively prevent publication based on content.

In exceptional cases, such as when a demonstration may pose a threat to public order, permission for the activity may be denied by competent authorities (but not based on the content of the speech, a matter we will return to later). In special circumstances, in matters of security, government agencies, such as the Security Service, may, proactively and with great caution, undertake informational measures directly aimed at publishers.

Additional exceptions apply to the conduct of general elections, during which there is a prohibition on propaganda near polling stations, which is punishable by law. Special regulations also exist to protect election officials from intimidation. Furthermore, receiving foreign support is a criminal offense if it influences public opinion regarding the fundamental principles of the state or national security.

Legal Framework for Cyber Threats

In legal terms, Swedish laws govern information and cybersecurity, and a rich array of national legislation and various EU directives exist in this field (more on these in section 6). An in-depth review of these laws would require a more comprehensive report; however, it can be noted that both national and European legislative activities have been extensive from 2016 onwards, likely attributed to increased awareness of cyber threats in general. Swedish information and

cybersecurity legislation generally aim to enhance society's overall resilience against all forms of IT-related incidents, and perhaps the exception of the broader Security Protection Act, are not aimed specifically at the threat from antagonistic cyber threat actors.

The distinction between wartime and peacetime, and between external and internal threats, is also reflected in cyber threat legislation. The Swedish Armed Forces have cyber defense units organized for wartime purposes to defend the nation against cyber-attacks, while the police investigate IT crimes such as data breaches or cyber fraud. Qualified IT attacks on critical Swedish infrastructure are investigated by the Security Service. The cyber arena transcends national borders and delineating between internal and external threats can be challenging. It can be difficult to attribute an attack to a specific actor or country, and Swedish criminal law requires a suspect, i.e., the person committing the cybercrime, to initiate a preliminary investigation to unlock investigative tools and coercive measures. It is also technically challenging to prosecute cybercrime perpetrators, especially if the perpetrator is a foreign state or state-sponsored actor with limited opportunities for international legal assistance.

Screening of Foreign Direct Investments

As mentioned earlier, no specific Swedish legislation has been explicitly enacted to address hybrid threats or any other definition of actions associated with hybrid threats in a broad sense. However, a law for screening foreign direct investment was recently passed, which can be seen as a response to a specific type of hybrid threat activity. Along with previous and additional legislative changes under consideration, a relatively extensive legal framework has emerged to prevent foreign interests from jeopardizing Swedish security through acquisitions and investments.

Authorities like the Security Service have highlighted the issue that foreign actors have been able to acquire sensitive technology, infrastructure, and data relatively unhindered, often as a complement to intelligence gathering, in order to gain technological, military, or political advantages. Concerns have been raised that acquisitions or investments can be used for actions in hybrid or wartime scenarios (e.g., impacting energy supply). The first legal measure introduced to allow control of certain commercial activities was when the Security Service and the Swedish Armed Forces in 2021 were given the authority to stop the outsourcing of sensitive activities under the Security Protection Act. This followed the highly publicized Transport Agency scandal, in which driver's license information had been outsourced to an IT provider in Serbia. A prominent example of when the Security Service and the Armed Forces intervened in a commercial transaction was when the Chinese telecommunications manufacturer Huawei was stopped in 2020 from participating in the construction of the Swedish 5G networks, a decision that was upheld in civil court in 2021.

In September 2023, a Law on Screening of Foreign Direct Investments in Protected Activities was adopted by the Swedish parliament, effective from December 1, 2023. This law represents Sweden's implementation of European Parliament and Council Regulation (EU) 2019/452, which established a framework for screening foreign direct investments in the Union. A foreign direct investment in a protected activity must, before the investment is made, undergo a review by a government authority. The aim is to prevent foreign investments that could harm Sweden's security, public order, or public safety. Foreign direct investment can be prohibited or subject to conditions, if necessary, to protect Swedish security interests. Security interests include

activities covered by the Security Protection Act, critical infrastructure, and military equipment, as well as emerging technologies, critical raw materials, and personal data. Together with the Security Protection Act's provisions allowing the Security Service and the Swedish Armed Forces to block foreign subcontractors, a relatively extensive and far-reaching package of measures has now been developed to counter this type of hybrid threat. Notably, investments in media companies are exempt from the review system.

Furthermore, an ongoing investigation concerns control over the transfer and lease of property of essential importance to total defense. This investigation stems from the need to ensure that a foreign power cannot acquire land and facilities near defense-critical activities, a phenomenon that has been mainly discussed in the media concerning individuals and companies linked to the Russian state owning ports or land near coastal military protected sites.

Policy coordination, interagency cooperation, and information sharing

Overall Policy Coordination and Information Sharing
In Sweden, there is no central authority, agency, or structure for coordinating and sharing information related to hybrid threats. Instead, responsibilities are distributed among various government agencies, irrespective of the level of conflict. Government agencies have resumed planning for civil defense, with increased resources dedicated to countering cyberattacks and information influence. However, there is currently no specific strategy for countering hybrid threats.

The Swedish Civil Contingencies Agency (MSB) plays a particular role in civil defense and preparedness planning during peacetime and heightened readiness. The MSB is responsible for supporting the 60 government agencies divided into 10 preparedness sectors within the national preparedness system during peacetime and heightened readiness. Each preparedness sector has a sectoral authority responsible for leading and coordinating actions during peacetime crises and heightened readiness.

Within the government offices, several ministries are responsible for issues that fall within the scope of the hybrid threat concept, particularly the Ministry of Defense and the Ministry of Justice for their responsibilities in security policy matters and the direction of defense and police authorities, as well as the MSB. An ambassador-level envoy for hybrid threats was established within the Ministry for Foreign Affairs in 2018 although that role played no inter-departmental coordinating role or mandate. The absence of a centralized function for the coordination and management of hybrid threats may be attributed to the evolving nature of these threats, making it difficult to define what constitutes a hybrid threat activity. In addition, there have been few coordinated attacks, according to the definition of hybrid threats, that have been carried out against Sweden, as far as is known. As a result, the presence of hybrid threat to has been handled on a case-by-case basis by different government departments and agencies.

However, there are indications that hybrid threats are being elevated to a central place in the Swedish government. The establishment of the National Security Advisor on January 1, 2023 is a response to the deteriorating security situation. The National Security Advisor will coordinate, analyze, and align Swedish security policy as a whole. The creation of the National Security Advisor role represents a response to the deteriorating security situation. The advisor convenes

the Security Council every other week, which includes the Prime Minister, Defense Minister, Minister for Civil Defense, Justice Minister, Finance Minister, and the leaders of coalition parties. Hybrid threats, alongside cyber threats and the space dimension, have been highlighted by the advisor as areas requiring coordination, as they span multiple policy areas, ministries, and agencies. The advisor has offices for foreign and security policy, crisis management, strategic analysis, and intelligence, the latter accompanied by an intelligence council. This structure is probably the most comprehensive approach to creating a whole-of-government approach in security policy. However, it should be noted that the advisor and the offices are part of the government offices, and government agencies remain independent in their work, as stipulated by the Instrument of Government. Agencies cannot be directed by either the advisor or an individual minister, but only through collective government decisions such as budget directives or instructions.

Coordination in Psychological Defense

In Sweden, countering hybrid threat to such as disinformation and information influence is viewed as part of psychological defense. All government agencies are responsible for Sweden's psychological defense, including countering information influence campaigns. The Agency for Psychological Defense (MPF) is tasked with leading efforts to coordinate other agencies and provide support in countermeasure activities. During peacetime and heightened readiness, the MPF is responsible for coordinating and developing the activities of government agencies and other relevant authorities in psychological defense. Every authority is responsible for countering information influence, but the MPF coordinates the efforts of several agencies. Some complications may arise due to principles of responsibility and proximity, which stipulate that countering information influence at the municipal level, for example, should be carried out by the responsible municipal authorities (which may have limited expertise for this purpose), while the same type of activity has a regional or national dimension and can consequently be addressed at those levels as well.

In a somewhat dated survey from 2017, it was found that most Swedish government agencies have procedures for identifying information influence targeting their own operations. However, there were no coordination mechanisms between agencies or procedures for countering such activities. The MPF was tasked with proposing a structure for cooperation, which was partially reported in 2023. This report noted that a preliminary dialog had already begun with several agencies that could participate in a future cooperation structure within psychological defense. Four areas of cooperation were identified (military defense, civil defense, media and information literacy, and Sweden's image aborad), along with suggestions for which agencies should be involved in each area. Various levels of ambition for cooperation were proposed, ranging from voluntary cooperation between relevant agencies to government instruction to consolidate agencies into a more tightly coordinated structure. Other proposals were making MPF the sectoral responsible preparedness authority for psychological defense, and ultimately, establishing psychological defense as a distinct part of total defense, alongside civil defense (under which MPF currently falls under) and military defense.

Coordination in Cyber Threats

The area of cybersecurity has been extensively examined from a collaboration perspective in Sweden. In 2023, the Swedish National Audit Office (Riksrevisionen) reached discouraging conclusions in its review of the national cybersecurity strategy adopted by the former

government in 2017 and its implementation. More details on the shortcomings are discussed in section 4, but it should be noted that the work on cybersecurity within the Swedish government involves several ministries. The Ministry of Defense and the Ministry of Justice play a more prominent role, but between 2017 and 2022, up to nine different ministries, and in some cases several units within the same ministry, have been involved in cybersecurity matters to varying and overlapping extents. In the absence of clear political guidance and central authority for these matters, several interdepartmental working groups (known as "ida-groups) have been formed to coordinate national cybersecurity efforts. Riksrevisionen has called for a central hub for cybersecurity in government offices. The National Security Advisor has identified cybersecurity as a horizontal focus area where coordination, analysis, and control will be strengthened through the establishment of the advisory role.

The distribution of responsibilities at the ministry level is also reflected among the numerous agencies that are jointly responsible for cybersecurity, with none having primary responsibility for overall information and cybersecurity. The Swedish Civil Contingencies Agency (MSB) holds a unique position, as government agencies are obliged to report IT incidents to the MSB, which reports cyber incidents of a criminal nature to the police. The MSB is also responsible for issuing regulations on information and cybersecurity for government agencies, managing the Swedish Computer Emergency Response Team (CERT), and several national contact points for the EU's cybersecurity systems. Moreover, the MSB is the sectoral responsible preparedness authority for IT in civil defense.

There are numerous networks and working groups at the agency level that are focused on information and cybersecurity. Most of these are involved in ensuring information security in general, rather than addressing the perspective of antagonistic actors. An attempt to strengthen coordination against antagonistic cyber threats to the establishment of the National Cybersecurity Center (NCSC). In 2020, the agencies primarily following antagonistic cyber threat actors, namely the Swedish National Defense Radio Establishment (FRA), the Swedish Security Service, and the Swedish Armed Forces, were tasked with jointly establishing NCSC, together with the MSB. The initial purpose was to coordinate efforts to prevent, detect, and respond to cyberattacks and IT incidents; provide advice and support regarding threats, vulnerabilities, and risks; and serve as a platform for information exchange with private and public actors. Over time, cooperation expanded to cover more areas. Eventually, the Swedish Defense Materiel Administration (FMV), the Police Authority, and the Swedish Post and Telecom Authority (PTS) were also involved in the center's collaboration. However, the establishment process was marked by problems that can be attributed to the various agencies' independence, cultures, and lack of clear leadership over the center. Consequently, in May 2023, the government decided to place the center under the authority of the FRA.

Another collaborative structure with theoretical relevance to hybrid threats is the National Telecommunications Collaboration Group (NTSG), a voluntary working group consisting of agencies (including PTS and the Swedish Armed Forces) and telecommunications operators. The group collaborates to ensure the maintenance of telecommunications during disruptions, which is relevant for resilience against sabotage and cyberattacks.

Coordination in the Review of Foreign Direct Investments

It is highly likely that the Inspectorate for Strategic Products (ISP), which already serves as the national contact point for the European screening system, will be responsible for screening foreign direct investments. The new law stipulates that the screening authority should consult with other government agencies designated by the government. As we have seen in the aforementioned example of Huawei, it is likely that the Swedish Armed Forces and the Swedish Security Service are two prominent consultation authorities. On a side note, when ISP assumed its role as national point of contact for the EU regulation on screening of foreign direct investments, it was proposed by the then-member of parliament Pål Jonson, now the Minister of Defense, to enable the agency to direct FRA to conduct signals intelligence activities to support its mission, although this proposal has not been implemented. This initiative to empower ISP to request intelligence specifically for their missions may be interpreted as an indication of the importance of security policy that is being attributed to foreign direct investments.

Assessment and prioritization of hybrid threats

As there is no central function for coordination of the response to hybrid threats, there is also no, at least publicly described, unified national process for the assessment and prioritization of hybrid threats. However, a clearer process for assessment and prioritization from the government's side can be discerned since the establishment of the role of the National Security Advisor. The advisor is working on a new national security strategy intended to guide and direct ministries and relevant agencies. This strategy is expected to contain a vision, threat analysis, strategy with clear priorities, trade-offs, resource allocations, the government office's work, and relevant agencies. As mentioned earlier, hybrid threats have been mentioned as an example of areas that the advisor will coordinate. It should be mentioned that there has been a national security strategy previously too though that did not offer much guidance in terms of operationalization and coordination.

This doesn't mean that some form of prioritization is not taking place, however. Rather, it can be observed through the outcomes of various processes, statements, and initiatives. Considering this, the government's political agenda concerning certain threats can be interpreted because of work within the government and the government office, including considerations related to hybrid threats, such as in the run-up to the Swedish EU presidency in 2023 (see p.7). However, it is more challenging to elucidate the underlying process, which likely involves a combination of interdepartmental coordination processes within the government office, input from agencies, budget negotiations within the government budget, and initiatives prompted by events, global developments, or election promises.

An example of a process that is inaccessible to the public for assessment and prioritization is the direction of intelligence activities, where the government, through the Ministry of Defence, directs the Swedish National Defence Radio Establishment (FRA), the Swedish Military Intelligence and Security Service (Must), as well as the less prominent Swedish Defence Materiel Administration (FMV) and the Swedish Defence Research Agency (FOI). This is a closed process but presumably involves trade-offs between different priorities, which can be interpreted as the highest national assessment of the most significant threats. The same can be said about government decisions, appropriation letters, and budget allocations for specific initiatives. For instance, the National Center for Cybersecurity (NCSC) agencies have received increased funding

to strengthen their work, and the Civil Contingencies Agency (MPF) has been given specific tasks through instructions related to international cooperation.

The assessment of threats and their internal prioritization are primarily the responsibility of intelligence agencies, mainly FRA, Must, and the Security Service (Säpo). These agencies conduct intelligence activities and independently provide assessments to the government, government office, and other authorities. Currently, in Sweden, unlike, for example, the United Kingdom, there is no central body that synthesizes the reporting of various intelligence agencies into a national assessment. However, the National Security Advisor is expected to have an intelligence office and a corresponding national intelligence council, which theoretically could assume such a role. Intelligence agencies communicate certain events, developments, and general assessments in their publicly available annual reports. Based on these reports, there is relative consensus regarding the importance of hybrid threats and the types of hybrid threats highlighted (cyber, influence, intelligence activities, technology acquisition). The MPF also shares its assessments of threats and threat actors in the context of current events or crises. The NCSC has been expected to provide common cyber threat assessments but appears to have struggled to meet that vision. In the counterterrorism field, there has been a National Centre for Terrorism Threat Assessment since 2009, which synthesizes assessments from FRA, Must, and Säpo into a threat assessment, but similar mechanisms for hybrid threats or cyber threats do not exist.

Challenges and effectiveness in countering hybrid threats

As evident, there is no cohesive structure for the management of hybrid threats in a broad sense, neither at the government level, government office level, nor at the agency level. Therefore, it is challenging to provide exact answers to this question. However, by addressing the shortcomings that have emerged in the structures that do exist within general crisis preparedness, cyber threats, psychological defense, and screening of foreign direct investments, certain general assumptions can be made.

Legislative challenges

As previously stated, hybrid threats are managed within the framework of crisis preparedness during peacetime and heightened preparedness. This leads to challenges, such as collaboration between the police and armed forces when Sweden is subject to hybrid threats but not at war. Proposals and initiatives have been put forth by both the police and the Swedish Civil Contingencies Agency (MSB), as well as in the parliament, calling for an adaptation of legislation to allow the Police Authority to request additional peacetime assistance from the Swedish Armed Forces in more cases than just terrorist acts and helicopter transportation. Perhaps hybrid threats, in their entirety, need to be recognized as a condition running alongside the classical conflict scale (peace, heightened prepareness and war).

Another challenge is that an open society enables disinformation, while effective tools to counter such information are lacking due to freedom of speech and information, regardless of whether the sender is a threatening foreign state actor or not. Preventive restrictions can only be made on the basis of the local effects of an expression of opinion, not its content. An ongoing example of this inherent conflict is the series of public burnings of the Quran by activists during the summer of 2023, which caused condemnation from many Muslim countries, including

Turkey. Freedom of expression clashed in this case with the national security interest of swiftly being approved as a member of NATO, a process that was, and still is, dependent on ratification by the Turkish parliament. In one case, the police authority attempted to stop a burning of the Quran, citing that this action could lead to an increased terrorist threat. This argument was subsequently rejected in a legal review because restrictions on freedom of assembly can only be made due to security risks associated with the actual demonstration. The possibility of restricting freedom of assembly on the grounds of national security, i.e., widening the possibilities for preventing an expression, is currently under consideration.

In the field of cybersecurity, several aspects of legal complications have arisen, which are quite well highlighted through the establishment of the National Center for Cybersecurity (NCSC). This includes issues related to the handling of personal data between different agency IT systems or aspects of confidentiality (e.g., source protection in intelligence activities). Another challenge is that some agencies responsible for cybersecurity are intelligence services, some are law enforcement agencies, and others are responsible for civil preparedness. Different legal frameworks for their operations and varying cultures of collaboration and information sharing can, in the absence of central coordination, lead to overlooking connections between seemingly unrelated events and be the first point of contact for incidents that may not initially appear to be linked to an adversarial actor. This phenomenon likely applies to cyber threats and other hybrid threats.

Lack of strategic governance and clear responsibility

The Swedish National Audit Office's review of national cybersecurity efforts has shown significant shortcomings regarding strategic governance at the government and government office levels. This can be attributed to the lack of trade-offs and prioritization. In the absence of a clear policy in the field, ministries and agencies work based on their respective goals and priorities, divided responsibilities, and domains, which has an impact at the agency level and is further reinforced by the independence of these agencies and sometimes overlapping, sometimes widely differing focuses. The Swedish National Audit Office also notes a lack of specific targets and budget allocations in the government's cybersecurity strategy. Furthermore, the many agencies involved in cybersecurity work have different tasks and mandates, and there appear to be varying perspectives on the focal points. As mentioned earlier, the starting point for information and cybersecurity is not solely the threat from antagonistic actors. Although baseline information security cannot be disregarded, the NCSC's mission is specifically to counter antagonistic cyber threats. On occasion, the MSB has criticized the intelligence agencies for being too focused on the activities of state-supported actors and not on society's information and cybersecurity in general. The Säpo, FRA, and Swedish Armed Forces have also excluded MSB from a smaller forum for protection against serious IT threats to the NCSC framework.

Psychological defense and mechanisms for reviewing foreign direct investments have not yet been subject to the same level of scrutiny as cybersecurity efforts, but it is reasonable to assume that certain challenges related to strategic governance and agency collaboration are similar to those in the field of cybersecurity.

Throughout, it can be noted that several agencies are tasked with **coordinating** cooperation and working together. However, there is a lack of responsibility for **leading** the response to hybrid

threats, which leads to the question of who would be in charge in an elaborate peacetime hybrid threat scenario orchestrated by a foreign threat actor with domestic implications in Sweden.

The role of the private sector

The private sector plays a crucial role in societal crisis preparedness, but its role is largely unregulated or under development. The Swedish Civil Contingencies Agency (MSB) informs companies about their role in crisis preparedness and enlightens them about hybrid threats. The importance of collaboration with the private sector is consistently emphasized in the guidance of initiatives related to hybrid threats, especially in the field of cybersecurity, where the private sector is described as central, given that networks and infrastructure are privately owned.

NCSC was already instructed to collaborate with the private sector at the time of its establishment, but as late as the spring of 2023, the private sector had not yet been involved in the development of NCSC. Representatives of the private sector have criticized the lack of a clear contact point and home for cybersecurity issues in the government office, a lack of information from the state/NCSC on cybersecurity, and a perceived lack of interest from the state in information from private actors. At the same time, state representatives argue that there is an overestimation of the assistance that the state can provide to the private sector. However, the cybersecurity field, contrary to the perception of lack of collaboration, is likely the security policy area with the highest level of interaction between the state and the private sector through several sector-specific working groups initiated by MSB (e.g., for the healthcare sector and the financial sector). The existence of these working groups naturally says nothing about the quality or results of the work.

One step, unrelated to NCSC, that was taken to provide private sector entities with better cybersecurity capabilities was when, in 2022, the FRA was given the authority to offer cybersecurity advice and expertise to companies important to critical infrastructure (such as in the financial sector) alongside government agencies and state-owned companies.

Within psychological defense, the importance of the private sector has also been articulated, especially because the press and media are largely private organizations. MPF is mandated to support media companies, and the agency is also meant to strengthen the private sector's capabilities. The extent of this support has not been clarified, but it likely primarily involves MPF's extensive information activities. As mentioned in point 1, in exceptional cases, the Swedish Security Service can inform publishers about the security aspects that may follow a publication. In a report on hybrid threats published 2020, FOI has, in the form of a fictional hybrid threat scenario, floated the idea that the government, through MPF, should use contracted communication agencies to respond to disinformation and information influence in a crisis. This idea is reminiscent of Cold War total defense planning, when journalists and communicators in private media companies could be assigned to ensure access to accurate information.

Regarding the very recent introduction of a review system for foreign direct investments, there is a lack of experience in how collaboration between the state and the private sector works in practice. However, the introduction itself is, by definition, a tool for interacting with and even exerting control over private business interests and an intervention in business operations.

Representatives of the private sector have warned of increased costs and other negative effects of the review system on unproblematic investments.

Effects of EU and NATO membership

Sweden shares its security challenges with other EU members, and its foreign policy has a strong EU dimension. Sweden is also covered by the mutual defense clause (in the case of armed aggression) of the Treaty of the European Union and the solidarity clause of the Treaty of the Functioning of the European Union (in case of a terrorist attack or a natural or man-made disaster).

Regarding hybrid threats, Sweden has actively sought participation in EU and NATO forums and projects (see more in point 8) to enhance its own and its partners' capacity against hybrid threats. Before Sweden's EU presidency, Sweden declared that hybrid and cyber threats, as well as undue information influence, would be prioritized issues during the upcoming six months. It emphasized the importance of EU and NATO cooperation in this area and announced ambitions to use the experiences from the establishment of the MPF to strengthen efforts against undue information influence in Europe, enhance the EU's cyber diplomatic toolbox, and establish rapid response teams to address cyber threats. Sweden's capacity to counter hybrid threats increases through EU and NATO membership because information sharing about events in member states can be used to prepare other member states for similar events. As far as cybersecurity is concerned, Sweden also participates at the expert agency level in European organizations and working groups, such as the European Union Agency for Cybersecurity (ENISA). Sweden ratifies and implements the EU's cybersecurity initiatives (e.g. DORA, NIS2, CRA), although not all have been fully implemented yet. While Sweden's cyber capabilities are enhanced through the implementation of the EU framework, industry representatives have articulated concerns that a certain tendency toward overregulation creates administrative procedures that outweigh the benefits. Furthermore, the Swedish National Audit Office has noted that within the Ministry for Foreign Affairs, there is a perception that the government office, due to inadequate resources and internal organization, becomes reactive in international information and cybersecurity cooperation. This has led to Sweden not being able to influence these issues in a more favorable direction. The reason for this deficiency is said to be a lack of coordination and prioritization within the Ministry for Foreign Affairs and the government office as a whole. It also appears to be challenging to equip Swedish delegates with national processed threat to as support for international meetings.

The application for NATO membership is a significant measure to enhance Sweden's security in itself, including against hybrid threats. Furthermore, NATO's article 4 ´provides member states, as well as partner nations, with the political instrument to raise issues for consultation in the North Atlantic Council, where, for example, hybrid threat campaigns can be addressed.

Lastly, both the EU and NATO are building capabilities to resist and recover from disturbances related to interdependent vulnerabilities. This is referred to as *forward resilience* and aims at increasing member states' capabilities to anticipate, preempt, and resolve disruptive challenges to vital societal functions. The EU and NATO are also exploring ways to work more effectively together in this area.

International cooperation on hybrid threats

Sweden has established a special envoy for international cyber issues within the Ministry for Foreign Affairs since August 2023. The special envoy's task is to represent Sweden in the EU, UN, and NATO and to work for Sweden's interests in the cyber domain. Additionally, there is an ambassador within the Ministry of Foreign Affairs responsible for hybrid threat to. The former position is informally described as more focused on overarching matters related to international technology issues, while the latter is more focused on antagonistic threats.

Swedish authorities and ministries collaborate internationally on bilateral and multilateral issues. This applies to the field of cybersecurity, as well as for the MPF and other agencies involved in hybrid threat issues. However, it is challenging to assess the extent of this collaboration and how much of it pertains specifically to hybrid threat issues. In many cases, particularly within defense intelligence services, international cooperation is subject to confidentially laws. To the extent that these agencies comment on their international collaboration, they describe it as essential for fulfilling their tasks, and it can be assumed that hybrid threats as a phenomenon or specific hybrid threat incidents are subject to this collaboration.

Information exchange is also a component of international intelligence cooperation, but the extent, significance, and outcomes are not publicly disclosed. Säpo tends to be the least secretive of the Swedish intelligence services, having stated publicly that cooperation with its counterparts in the Nordic countries, in the EU and in the United States is particularly close. Europol and the multilateral Counter-terrorism group are also mentioned publicly as important forums for Säpo. The Armed Forces are contributors to the EU's various intelligence functions, such as INTCEN and INTDIR. In some cases, government agencies are given specific, and publicly disclosed, mandates by the government to cooperate with particular states. For instance, MPF has been tasked through government directives to collaborate with Ukrainian authorities. Sweden also contributes personnel or funding to the following international collaborative bodies in the field of hybrid threats.

- European Centre of Excellence for Countering Hybrid Threats
- EU Hybrid Fusion Cell
- The Cyber and Hybrid section of the International Staff's Division for Emerging Security Challenges at NATO HQ
- Nato Strategic Communications Centre of Excellence
- EU European External Action Service Stratcom Task Force
- Nato Cooperative Cyber Defense Center of Excellence

Lessons learned from Sweden's management of hybrid threats

As we have seen, only three hybrid threat-related areas appear to have been addressed through more structured approaches. It is likely that lessons learned from these areas may serve as examples for implementing hybrid threat to in other existing or future hybrid threat to. That

said, and somewhat surprising given the attention given to hybrid threats in the security policy discourse, very little appears to have been published in terms of lessons learned from hybrid threat scenarios and how these lessons have been used to increase resilience. None of our interlocutors could recall any findings from past campaigns that had been implemented into the new policy.

Part of the reason is probably that hybrid threats have very rarely been problematized in a broad sense. There are few openly documented or published experiences of a national response to hybrid threats in the sense that it involves a concerted campaign of various actions aimed at achieving the goals of an antagonistic state. Very likely, lessons learned in this regard, if existent, are being handled internally by the relevant agencies and concern their specific role in a hybrid threat scenario. These findings have generally not been shared with the public.

Openly available experience narratives related to what could be parts of a hybrid threat to often involve isolated events or specific tactics, such as disinformation or a cyber-attack. These depictions are often academic or journalistic. For example, research institutions such as the Swedish Defence Research Agency (Försvarets forskningsinstitut) and the Swedish Defence University (Försvarshögskolan) produce reports on hybrid threat activities. These reports are usually commissioned by relevant authorities such as the MPF or the Police Authority. This implies that these lessons learned are at least being requested and probably consumed, but it is unclear to what extent they are implemented for capacity building.

It is worth repeating that the national security advisor's office could be a vital component in implementing lessons learned into new policy.

Literature

Laws

Freedom of speech and expression
Kungörelse (1974:152) om beslutad ny regeringsform
Yttrandefrihetsgrundlag (1991:1469)
Tryckfrihetsförordning (1949:105)

Military support to police operations
Lag (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning
Förordning (2017:113) om Försvarsmaktens stöd till polisen med helikoptertransporter

Civid defense and protective security
Förordning (2022:524) om statliga myndigheters beredskap
Säkerhetsskyddslag (2018:585)

Screening of foreign direct investments
Lag (2023:560) om granskning av utländska direktinvesteringar
Europaparlamentets och rådets förordning (EU) 2019/452 av den 19 mars 2019 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen

Establishment of an agency for psychological defence
Förordning (2021:936) med instruktion för Myndigheten för psykologiskt försvar

Research reports and articles

Advokatfirman Vinge, 2023; Ny lag om granskning av utländska direktinvesteringar
FOI, 2020; "Strategisk verktygslåda mot hybridhot"
FOI, 2023; Rättsligt ramverk för bemötande av informationspåverkan
FOI, 2023; "Att bemöta påverkan mot genomförandet av allmänna"
Fägersten, Björn, 2017; Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence

Government investigations and agency information

Reform of civil defense
Regeringskansliet, 2017; Motståndskraft Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025
Myndigheten för samhällsskydd och beredskap 2023; Företagen är en viktig del av beredskapen
Myndigheten för samhällsskydd och beredskap; 2023; Strukturreform av krisberedskap och civilt försvar

Establishment of an agency for psychological defence
Myndigheten för psykologiskt försvar, 2023; Struktur för effektiv samverkan för det psykologiska försvaret
Myndigheten för psykologiskt försvar, 2023; Vårt uppdrag
Statskontoret, 2017; Myndigheternas arbete med psykologiskt försvar

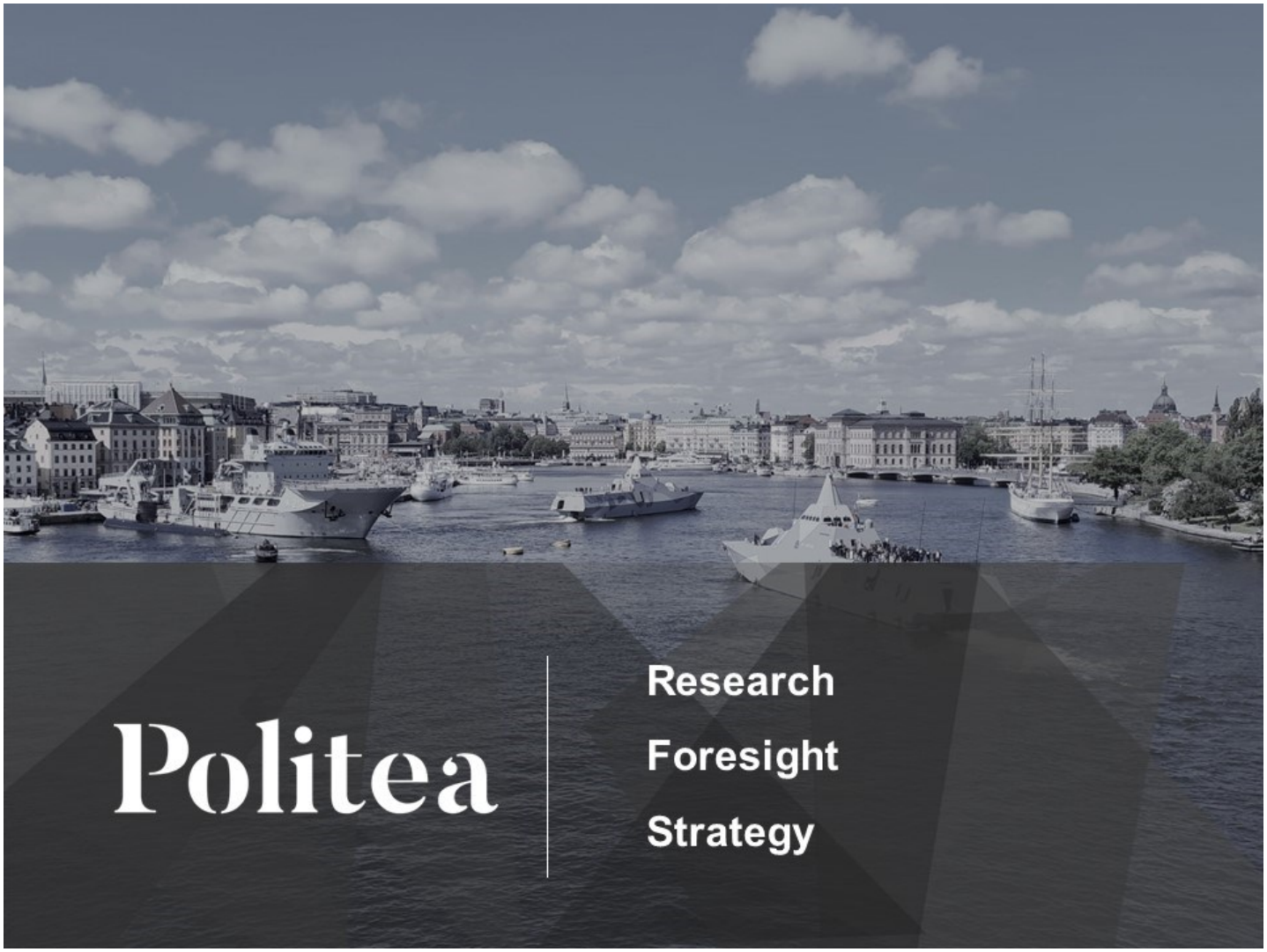
SOU 2020:29; En ny myndighet för att stärka det psykologiska försvaret
Ekonomistyrningsverket, 2023; "Regleringsbrev för budgetåret 2023 avseende Myndigheten för psykologiskt försvar"

Screening of foreign direct investments
Inspektionen för strategiska produkter, 2022; ISP - Om uppdraget
Inspektionen för strategiska produkter, 2022; ISP föreslås bli granskningsmyndighet
Regeringskansliet, 2018; Granskning av Transportstyrelsens upphandling av it-drift
Regeringen 2022; Kontroll vid överlåtelse och upplåtelse av egendom av väsentlig betydelse för totalförsvaret
SOU 2021:87; Granskning av utländska direktinvesteringar

Cybersecurity
Försvarsmakten 2023, Försvarsmaktens cyberförsvar
Försvarsmakten, 2016; Försvarsmaktens Handbok IKFN Hävdande av vårt lands suveränitet och territoriella integritet
Polismyndigheten, 2023; It-relaterade brott - lagar och fakta
Riksrevisionen, 2023; Regeringens styrning av samhällets informations- och cybersäkerhet
Myndigheten för samhällsskydd och beredskap, 2023; Policyöversikt Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete

Yearbooks from the intelligence- and security services
Säkerhetspolisen, 2023; Säkerhestpolisens lägesbild 2022-2023
Försvarets radioanstalt, 2023; FRA:s årsberättelse 2022
Försvarsmakten, 2023; Militära underrättelse- och säkerhetstjänstens årsöversikt 2022

Speeches and statements
Speech by Henrik Landerholm's on the establishment of the National Security Advisors office 10 January 2023
Speech by Foreign Minister Billström on Sweden's priorities for the EU Chairmanship 9 January 2023
Riksdagen, 2020; Motion : Sveriges förmåga att stå emot hybridhot
Utrikesdepartementet, 2023; New Special Envoy for Cybersecurity



About Politea

Politea is an analysis company focusing on international political risk, geoeconomics, and technology, based in Stockholm, Sweden. With research, foresight, and strategy development, Politea helps companies and authorities to navigate in an increasingly turbulent environment and position themselves for the future.

About the report

This is a public version of a report commissioned by The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). The Hybrid CoE has the full right to draw on any analysis of the report for their comparative work in the field.

Authors:

Dr Björn Fägersten. CEO Politea

Jens Holzapfel. Security and intelligence professional with 20 years of experience from Sweden's defence and national security community.

Published in October 2023