Myndigheten för
samhällsskydd
och beredskap

https://www.msb.se/sv/aktuellt/utlysning-av-forskningsmedel/

Call for research funding

Automated and autonomous cyber security

Table of contents

If the call text has changed after publication, the changes are listed here:

Date	Revision

Call for research funding - Automated and autonomous cyber security

Brief outline

The Swedish Civil Contingencies Agency (MSB) intends to fund research in the area of Automated and Autonomous Cyber Security.

The call amounts to a total of SEK 20 million. MSB provides full cost coverage for direct costs linked to the research project. Universities and research institutes are eligible to apply for the grant.

The following dates apply to the call:

Opening date:	2020-06-08
Application deadline:	2020-08-21
Last decision date:	2020-11-13
Suggested project start:	2021-01-01

MSB estimates that two to three projects can be granted. The projected duration is approximately five years.

MSB reserves the right to change the call text until two weeks before its closure.

Project proposals will be reviewed by the MSB and affiliated researchers.

Contact persons for the call:

Erik Sundström, call manager
+46-10-240 5371
erik.sundstrom@msb.se

Johan Turell, senior analyst
+46-10-240 4155
johan.turell@msb.se

MSB's research mission

MSB is responsible for matters concerning civil protection, public safety, emergency management and civil defence, to the extent that no other authority has the responsibility. The responsibility refers to measures taken before, during and after an accident, crisis, war or danger of war.

Knowledge development plays a strategic role in MSB's work for a safer society. As research is one of the most important ways of developing knowledge, MSB has the task of directing, ordering and ensuring the quality of research conducted on its behalf.

MSB funds needs-oriented research through thematic grants. The aim is to generate practical applicable research findings that will lead to an increased ability to solve societal problems. MSB research covers a wide field, encompasses several disciplines and is carried out in a cross-sectorial and international context. The aim of the research funding is to lead to new understanding, new methods, better decisions or new products/services.

In order to stimulate research on civil contingencies MSB allocates approx SEK 120 million annually to a variety of research activities, for example, funding for major research programmes, individual projects, and competence and structural support.

Background and general scope

Introduction to the call

A digitized society is dependent on functioning network and information systems. Lack of adequate information and cyber security can result in a more exposed and vulnerable society. That, in turn, may lead to high economic costs for both individuals and organizations, disruptions in essential societal services, exposure of sensitive information and a generally vulnerable society.

With advances in autonomy technologies and automation, opportunities and challenges arise for information and cyber security. Through machine learning and other technologies, systems are able to, on their own, gradually strengthen their ability to detect, monitor, analyse and respond to both traditional threats, risks, vulnerabilities and incidents and new threats and risks that are in themselves a result of technological development.

MSB sees that research in and for such systems and their possible applications is needed, and that they are considered to have great potential in, for example, the protection of critical infrastructure and socially important activities.

However, autonomy technologies and automation may also either be employed to (intentionally) do harm or to (unintentionally) cause harm as a by-product of their application. MSB considers research in this field to be considerable importance in order to strengthen understanding of the emerging risk landscape.

MSB considers research in the field of autonomy and automation of strategic importance, and sees a great potential for enhancing information security in critical infrastructure and essential services.

The call

This call for research funding addresses those who wish to realize a research project in the field of Autonomous and Automated Cyber Security. The project coordinator must be a university or research institute.

The aim of the project is to contribute to the development of knowledge about and to stimulate to new practise for autonomous and automated cyber security.

When assessing project applications, MSB will place particular importance on the prospects for *both* generating excellent research *and* generating results that may be further developed and used in society. Examples (the list is not exhaustive) of such results may be new technologies or new areas of application for existing technologies, decision and policymaking support, frameworks, design principles, tools, guides, services, standards, databases, training, etc.

Scoping principles

MSB follows the all hazards approach in all of its missions. MSB therefore considers cyber security, broadly defined, as protection of the availability, confidentiality and integrity of information systems, networks and information assets against incidents, threats and vulnerabilities no matter their cause or nature. Also in line with the all hazards approach, MSB considers a threat (broadly defined) to be something (anything) that causes and incident, or something (anything) that causes unwanted consequences as a result of an incident. Correspondingly, MSB considers a vulnerability (broadly defined) as a lack of something (anything) that could prevent an incident from occurring, or as a lack of something (anything) that could prevent unwanted consequences as a result of an incident. MSB does not limit cyber security to incidents caused by antagonists, or to antagonistic threats that cause incidents. Research proposals, within the scope of the call, relating to protection against natural threats, system errors and human mistakes are therefore as valid as research proposals relating to protection against antagonistic threats.

In view of the above, MSB considers the overall theme of the call to be about how autonomy technologies and automation strengthens (or may strengthen) as well as challenges (or may challenge) cyber security. Project proposals may either encompass present strengths and challenges or future strengths and challenges or both. Research proposals on present strengths and challenges shall demonstrate existing (and independently verifiable) cases of such strengths and challenges. Research proposals on future strengths and challenges shall demonstrate a credible case explaining why those potential strengths or challenges will come to be strengths or challenges in the future.

MSB considers autonomous and automated cyber security to be of particular importance for actors engaged with critical infrastructure and within essential services sectors. The sectors are:

- Energy supply
- Food and water supply
- Transports
- Health care and care
- Financial services
- Information and communication services
- Protection and security

MSB considers integrated research approaches to be of particular interest. Research into autonomy technologies and automation that take into account the legal and policy landscape may sometimes lead to conclusions and results that are more relevant, especially in terms of post research use of those conclusions and results.

Possible subthemes

Within the scope of the overall theme, MSB sees a wide space for research. Research proposals will naturally be orientated to a, or a number of, subthemes. Applicants are welcome to propose research in any of the subthemes listed here, or to propose subthemes of their own.

[Text to be further developed here]

- Privacy compliant intrusion detection and forensic analysis
- Vulnerability and threat analysis
- Efficient human to machine and machine to human cooperation in cyber security
- Intelligent malware and intelligent "protection ware"
- Automated or autonomous social engineering and countermeasures
- Anomaly detection
- Resource management
- Situational awareness
- Security for autonomy technologies and automation (so that the systems we use for greater security cannot be hijacked or disabled)
- Issues pertaining to development and maintenance of trust

Resources to draw upon

Technologies and techniques developed within the research programme which receives the grant will be required to be demonstrated, for instance through simulations or exercises. To this end, the MSB may provide access to the Swedish National Cyber Range in Linköping. The facility may also be utilized as a test bed and for experimentation purposes.[1]

Timeframes

The call opens on 8th of June 2020 and the full research application must be submitted to MSB by the 21th of August 2020.

[1] https://www.foi.se/en/foi/resources/crate---cyber-range-and-training-environment.html

MSB’s decision on which proposals the agency intends to fund can be expected at the latest by the 13th of November 2020. Funded projects should start 1st of January 2021.

Selection and preparation

The call is made in one step. The research applications will be reviewed in two phases. The first phase will consist of an internal assessment. Those applications who pass the first phase will go on to the next phase and be reviewed by scientific expertise in relevant areas.

MSB reserves the right to contact the applicant for discussion and information collection.

Criteria for assessment

In the assessment of the research applications, both expert administrators at MSB and external scientific expertise will participate.

The following criteria will be applied:

1. Needs-based research – The extent to which the research proposal is based on identified problems, challenges or issues in the practical field of information and cyber security.

2. Relevance for MSB – The extent to which the research proposal reflects the call text’s scope and aim. How well is the project expected to benefit MSB’s field of responsibility regarding information and cyber security.

3. Scientific quality – The extent to which the scientific problematization is able to frame and drive scientific excellence, and the extent to which the application and its proposed project(s) are in a position to produce scientific excellent results. The assessment of the scientific quality takes into account, among other things, novelty, problems, method, communication and applicants' competence. In situations where two research applications are considered equal in terms of need and relevance, scientific quality should be prioritized.

4. Subject matter expertise

5. Reciprocity – The extent to which the project plans for dialogue with MSB. Each research project is linked to a field of expertise within MSB and is given a project supervisor who is tasked with following the research. Larger projects have a steering and a reference group attached to the project.

6. Dissemination and utilization of results – The extent to which the project plans for the results of the research project to be used in different ways for practitioners responsible for information and cyber security; at policy and operative level. For example, the results can

sometimes be translated into education, evaluation, training and development activities.

7. Contextualisation – The extent to which results are developed in a way that enables society to make use of them after the research project has been concluded. If a research project develops a new technology that requires great amounts of personal information, then showing that legal requirements following from the GDPR has been met, and that using the technology does not impose any particular legal risk in that sense, would be an example of contextualisation. Another example of contextualisation would be if a new technology that faces "black box" challenges and requires trust to generate its intended effect has been developed, and the project has found a way of meeting that challenge so that trust can be maintained.

8. International perspectives – The extent to which research is conducted in international collaboration, the extent to which results are relevant beyond a particular country and the extent to which international aspects are taken into account in the research (such as whether technologies based on standards employed in certain part of the world are applicable to other parts of the world). Civil Contingencies in general and research in this area in particular has an international and a transnational dimension.

9. Gender equality, ethics and diversity – The extent to which the research is safe, ethical and promotes equality. To achieve the latter, a norm-critical perspective is needed in both project planning and project implementation. A norm critical perspective is about identifying, questioning and challenging norms linked to the protected grounds of discrimination in order to create inclusive, sustainable solutions.

Design of the application

It is important to note that all documents sent to the MSB are public, as per the Swedish constitutional principle of public access to official records. If an external party requests access to a document in MSB's keeping, the agency will make a decision on whether the there are grounds, as per the Public Access to Information and Secrecy Act, to withhold the information. If there are no such grounds, the information will be provided to the external party.

The complete research application is submitted via MSB's web-based application system. Visit https://etjanst.msb.se/e-tjanster/

The complete research application for MSB should be written in Times New Roman, 11 points with single line spacing and consist of the following:

- A project description of the research to be conducted within the intended project. In the description, the research front, problem statement, relevance, need of the project, project objectives, method of implementation, expected effect, target groups and communication will be described. (max 8 pages including reference list)

- A description of the existing research environment with an overall proposal for organizing and staffing the research. This should also include a description of existing skills and networks related to the environment (max 2 pages)
- CV with publication list for main applicants (max 7 pages, totally).
- CV for all co-applicants. (max 2 pages/co-applicant)
- General timetable (annex)
- Budget - Project budget is written in Excel, and is submitted with the application as an attachment. It should contain costs for salaries, employee benefits and overhead representing the total amount applied for.
- Salary costs - enter information salary costs per person.
- Other costs - specifies the other costs that will be incurred in the project. Specify on different cost types such as travel expenses, allowances or communication / dissemination costs.

Incomplete applications are not considered.

Formal requirements and certain restrictions

MSB's formal requirements for research applications are:

- The main applicant must hold a PhD and belong to a Swedish educational university or research institute.
- The project coordinator (a researcher) must work at least 15% in the project.
- Co-applicants share of the project's total time shall amount to at least 10%
- The proposal must be approved by a person authorized to sign for the firm at a university or research institute.
- All applicants must approve the handling of personal data according to Swedish law and the European Union General Data Protection Regulation.
- The research institutes applying for grants must demonstrate documented and relevant competence in the following areas:
    1. Cyber security
    2. Any and all technologies as well as policy or other areas that will be studied or developed during the course of the project
    3. Sector-specific knowledge (if the proposed project is set to examine sector-specific challenges or capacity development)

4. Innovation and development capacity to convert research results or collected data into public databases, products, services, standards, policy or decision support, etc.

To consider:

- MSB provides full cost coverage for direct costs linked to the research project. Enter the percentage for overhead mark up your university / institution applies.
- Equipment is funded only in specific cases. Premises for the research project should be included in the overhead mark up.

Additional information

Information on MSB's research activities can be found at:

- https://www.msb.se/en/about-msb/our-mission/research/ (English)
- www.msb.se/forskning (Swedish)
- www.msb.se/sv/aktuellt/utlysning-av-forskningsmedel/ (Swedish)

For further guidance on this call are more reading at (in Swedish):

- Investering i kunskap för ett säkrare samhälle – MSB:s strategi för forskning och utveckling https://rib.msb.se/filer/pdf/28834.pdf