Call for Cyber-Security Research Proposals

The Ariel Cyber Innovation Center has set its main goals to be the promotion of world-class cyber security research at Ariel University and the development and promotion of world-wide leading cyber security researchers. With these goals at hand, the Ariel Cyber Innovation Center is soliciting proposals for funding research projects in cyber security. The emphasis will be on innovative and forward-looking research. This should also assist in establishing the Ariel Cyber Innovation Center as a world leader in cyber security research.

Possible research topics include (but are not limited to):

- ✓ Systems security (including network security, mobile systems security, web systems security, cloud security, OS security, storage security, and firmware security)
- ✓ Hardware and embedded systems security
- ✓ Cybersecurity oriented cryptography and cryptanalysis
- ✓ Applied multiparty computation
- ✓ Applications of artificial intelligence and related fields (such as machine learning, natural language processing, or decision making) to cyber security (including applications such as vulnerability testing, detection of anomalous behavior of malwares, adversarial machine learning, privacy, etc.)
- ✓ Security analysis and security measurements (such as measurement of fraud, malware, spam, resiliency, or human behavior)
- ✓ Cyber Security aspects of physical systems, national infrastructures, and the Internet of Things (IoT)
- ✓ Human interaction and usability aspects of cyber security
- ✓ Privacy and personal data in cyberspace

The call is open to all the active academic staff at Ariel University as well as to external researchers who wish to be part of the Ariel Cyber Innovation Center.

Funding will be based on the regulations of the Center and can be used for supporting graduate students, post-doctoral fellows, academic visitors and research assistants. Funding can also be used for travel, literature, and equipment. The amount of funding will be comparable to that of ISF grants.

There are three types of research grants: regular, exploratory and travel. Proposals should clearly state the track they apply for, and the duration of the proposed research.

1) **Regular Research Grants (RRG):** These are regular research grants, for a period of up to 3 years (continuation after the first year will be subject to a review process). The proposals should contain:
   - ✓ Letter of Intent - A two-page description of the proposed research and its relevance to the current call. Additional supporting material can be submitted and will be evaluated at the discretion of the referees.
   - ✓ CV(s) and list of relevant publications of the principal investigator(s).
   - ✓ A declaration of current support for the PIs from other sources.
   - ✓ A budget proposal.

   A selected few of the submitted proposals will advance to a **second stage**. The PIs of these proposals will be asked to prepare a more detailed proposal, close in spirit to the standard ISF proposal format. The committee will be inclined to favor proposals that present some type of collaboration, such as, international collaborations with foreign research groups, employments of foreign research students or postdoctoral researchers, and hosting a visiting scientists from abroad. The scientific committee will place particular importance on novelty, methodology and suitable for publication at a top-tier scientific venues.

2) **Exploratory Research Grants (ERG)**: These proposals should identify a relevant subtopic and define a short term program (for up to one year) for obtaining the required knowledge and personnel for designing a research program in this subtopic. The format of these proposals will be exactly the same as the first stage of regular proposals. There is no second stage for exploratory proposals.

3) **Travel Proposals (TP)**: These proposals are for short and long term visits overseas. A short-term visit can be to one of the top security conferences (IEEE S&P, ACM CCS, and Usenix Security), or to a top security lab. A long-term visit can be to a top security lab, and can include a summer internship, semester overseas, and so on up to 4 months. (Note that travel to other conferences and locations can be covered within regular research grants up to a cap of 10%.) Travel proposals can be submitted at any time (at least 6 weeks prior to travel), and should consist of a single page. There is no second stage for travel proposals. Notification will be given in two weeks.

A remark about the center's software team and administrative staff: The center intends to form a professional software team that will be of service to all members of the center. If you wish to utilize the services of this team for the purpose of the proposed project, then you should target an appropriate amount of the requested funding in your proposal for this purpose. In addition, research proposals should take into account the cost of the center's administrative facilities and the proposed budget should account to that.

Budget requirements: Proposals should include a detailed list of possible expenditure items. The budget should not include salaries for PI's. The following percentage caps *must* be fulfilled (for exploratory and regular research proposals):

- ✓ Fellowships for graduate students and postdocs: minimum 35% and up to 100% of proposal
- ✓ Scientific and technical staff (including center's software team): up to 65%
- ✓ Travel: up to 10%
- ✓ Equipment and literature: Up to 10%
- ✓ General expenses: Up to 5%
- ✓ Administrative staff of the center: At least 10%.

Grant Limitations: An individual researcher can be a PI in at most two proposals (not including travel proposals).

Important dates:

May 15, 2019	Submission deadline at 23:59
May 26, 2019	First round notification (RRG)
June 11, 2019	Final notification (ERG)
June 12, 2019	Full proposals due (RRG)
June 30, 2019	Final notification (RRG)

Additional information:
The grant application process, and the usage of the grants, are subject to the regulations of the cyber center. Note that funding by the cyber center does not qualify for "Tosefet Bet" from the university. The regulations document can be obtained upon request by writing to acic@ariel.ac.il (and will be posted online as soon as the center website goes up).

The academic committee reserves its discretion as to awarding the grants, their internal division, including the option of not awarding any grant in one or more of the above types. The committee's decisions will be final.

At the end of every year, project progress will be reviewed. If unsatisfactory progress has been made, then the scientific committee may recommend that the funding be halted for the second year.

PI responsibilities: PIs of winning proposals will be required to provide a short written report on the results of the funded research at the end of every six-month period of the funding term and a final report at the end of the term. Each report shall include the publications supported by the center. (The report after short-term travel grants can be in the form of an oral presentation or a blog post regarding the conference.)

In addition, PIs will be required to take an active role in the Center (Principal Research Associate). In particular, they will be required to give public presentations of their research, they will be expected to attend seminars and events, and be present in the center for a reasonable portion of their time.

The Ariel Cyber Innovation center should be acknowledged in all public presentations and publications related to the funded research with the following acknowledgement "This work was supported by the Ariel Cyber Innovation Center in conjunction with the Israel National Cyber directorate in the Prime Minister's Office."

For any additional information or inquiries regarding this call for proposals, please send a message to Dr. Amit Dvir amitdv@g.ariel.ac.il