NCR-TAU Joint Grant Call for Research Proposals on Cybersecurity, 2021

Organised by

With the support of

The Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University and Cyber Security Agency of Singapore (CSA) are launching a joint grant call, under the domain of Singapore's National Cybersecurity R&D (NCR) Programme and the support of Israel National Cyber Directorate (INCD). This is the second Call for Research Proposals (CFP) created by these partners, inviting academics from both Israel and Singapore to conduct joint interdisciplinary cybersecurity research. The program is seeking proposals on novel ideas and technologies to address challenges faced by Singapore and Israel pertaining to; Secure Smart Cities, Internet of Things, Behavioural Studies and Social Science of Cybersecurity and Policy & Governance of Cybersecurity. The research areas include*:

A. Advanced early warning and threat analysis, mitigation and response
B. Communications and connectivity security
C. Digital trust and security assurance
D. Behavioural, psychological, sociological and other human aspects of cybersecurity
E. Policy, strategy, decision making, law, rights and privacy aspects of cybersecurity
F. Organizations, formal processes, financial perspectives, insurance and more Interdisciplinary cyber aspects

*See Appendix A for the expanded list of topics.

The NCR-TAU Joint Grant Call is launched with contributions from multiple ministries and public agencies, in order to highlight the cybersecurity capabilities, research and technology needed to address national security, smart nation and critical infrastructure needs. The grant call has been created in order to encourage interdisciplinary cybersecurity research and to support research that has both transnational and deployable outcomes.

The research goals methodology and plan will be developed by the Singaporean and Israeli teams, while each of the teams will apply according the local CFP instruction.

The Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University fosters interdisciplinary scientific research on digital transformation and cybersecurity through operating a sizable research fund that awarded 95 research grants which support more than 300 researchers worldwide as well as organizing , the Cyber Week conferences.

ELIGIBILITY AND FUNDING TERMS FOR TEL AVIV UNIVERSITY

The research proposal must include both Lead PI's from Singapore and Israel according to each country eligibility.
Israeli Lead PI must be a Tel Aviv University Faculty member[1].

Budget item	% of budget
Scholarships, stipends, fellowships for students (PIs are not eligible)	minimum 35%; up to100%
Scientific and technical staff (wages)	0-65%
Travel expenses	0-10%
Equipment	0-10%
Miscellaneous	0-5%

TAU Faculty may request for up to 400,000NIS per year in funding for up to three years. [2]

SUBMISSION

Applicants must use the templates provided in the package for the Research Proposal:

NCR-TAU Full Proposal Template (Word)	**NCR-TAU Grant Quad Chart Template (PowerPoint)**	**NCR-TAU Grant Call Budget Template for TAU faculty (Excel)**

TAU-based researchers must submit the proposal online. Singapore-based researchers submit the proposal to NCR.

[1] Israeli lead PI can have faculty members from other Universities as part of their research team.

[2] Research funding and duration are subject to ICRC's decision and budget availability.

*** Please note that the guidelines stipulated in this document apply only to researchers submitting from Israel. Please also take note that submissions do not have to be made to both parties.

Submissions close on February 1st, 2021.

Grant awards expected in April 2021.

EVALUATION

The Blavatnik ICRC Steering and Scientific Committees evaluate the proposal according to:

- Relevance: fundamental and applied advances in cybersecurity and digital transformation.
- Scientific and technical merit: scale and magnitude of potential scientific contribution, innovation within a discipline, innovation resulting from an interdisciplinary approach.
- Feasibility: team composition, PI expertise

GRANT RECIPIENTS' OBLIGATIONS

- Participate in Blavatnik ICRC activities in Tel Aviv University, including the annual Cyber Week conferences, briefing dignitaries and delegations, etc.
- Acknowledge the Blavatnik Interdisciplinary Cyber Research Center at Tel-Aviv University and Israel National Cyber Directorate (INCD) in all resulting publications.
- Submit accurate and timely activity reports to the Blavatnik ICRC.

For further information, contact:
icrc@tauex.tau.ac.il

Appendix A: Research topics

A. Advanced early warning and threat analysis, mitigation and response

- AI-enabled threat intelligence research and analysis
- Advanced AI capabilities for next-generation Cyber Security Operations
- Hyperautomation of advanced threat analysis and attribution
- AI-enabled threat mitigation and remediation
- Defending AI against cyber-threats
- Cybercrime investigation (e.g. Law enforcement in cyberspace and cybercrime)

B. Communications and connectivity security

- Security of interconnected heterogeneous systems
- Security in massive IoT connections
- Supply chain threat mitigation
- Zero trust techniques in 5G network core and boundaries
- Security of data-in-transit
- Self-healing networks for automated remediation

C. Digital trust and security assurance

- IoT and edge computing security for Smart Cities
- Privacy preservation amidst dynamic data sharing
- Cybersecurity oriented cryptography and cryptanalysis
- Anonymization and sanitisation
- Quantum resistant encryption and quantum systems
- Security of data-in-transit in the age of quantum computers
- Transparency, explainability and auditability of AI
- Vulnerability discovery and software repair of embedded systems
- Hardware security design and evaluation for embedded systems
- AI-enabled red teaming
- Security of cyber-physical systems and critical infrastructure

D. Behavioural, psychological, sociological and other human aspects of Cybersecurity

- Human interaction and usability aspects of cybersecurity
- Users reaction to Cyber alerts and effective user based protection
- Societies adoption of technology and Cyber behaviours

E. Policy, strategy, decision making, law, rights and privacy aspects of Cybersecurity

- Cyber policy aspects - national and sectoral levels
- Cyber strategy: from foundational principles to detailed programs
- Regulation and legislation: national and international aspects
- Political and military aspects of Cyber warfare
- Civil liberties and Ethics in Cyberspace
- Privacy and relevant laws

F. Organizations, formal processes, financial perspectives, insurance and other aspects Cybersecurity

- Organizational aspects of Cybersecurity
- Cyber roles, structures, organizational processes and trends
- Finance and monetary systems in Cyberspace
- Cyber insurance for safer and trusted cyberspace