BLAVATNIK INTERDISCIPLINARY CYBER RESEARCH CENTER

Activity report 2018

CONTENTS

BLAVATNIK INTERDISCIPLINARY CYBER RESEARCH CENTER

EXECUTIVE SUMMARY: 2018 IN REVIEW

Blavatnik ICRC pursues a clear mission: creatinga more secure world through science. The key statistics and accomplishments of 2018 demonstrate: Blavatnik ICRC already delivers substantial value to our diverse stakeholders: scientists, professional practitioners, officials, entrepreneurs and investors.

- One hundred fifteen Principal Investigators and sixty- three Academic Visitors in Blavatnik ICRC.
- Eighteen new research grants awarded.
- Eight thousand participants from eighty countries came to our Cyber Week 2018 at Tel Aviv University
- Research articles with marked policy impact:
  - Prof. Gandal et al demonstrated pervasive fraud in Bitcoin, contributing to a U.S. SEC ruling to deny a Bitcoin-based ETF
  - Prof. Shavitt et al uncovered China Telecom's recurrent and massive Internet traffic rerouting, swaying global debates on Chinese espionage
- Over fifty scientific articles published across a wide gamut of disciplines.
- Secured new government funding for Blavatnik ICRC.
- Secured new commercial research funding from Tata Consultancy Services (TCS), India.
- Launched the Executive Education program to engage business and government leaders.

Scientific Research

The core activities are at the forefront of cutting-edge cyber research. The Blavatnik ICRC research portfolio grew to seventy-four cyber research projects across sciences, engineering, social science, law, business management and medicine. In 2018, we received thirty-one proposals in response to our Call for Proposals. Using scientific criteria, we awarded eighteen new research grants. Eighteen of the seventy-four will be completed by Q1 2019.

- Blavatnik ICRC funds seventy-four scientific research projects in total, directly supporting two hundred and fifty researchers across TAU's schools and faculties

The proposals accepted in 2018 demonstrate scholarly attention to new cybersecurity-related topics, as well as innovative scientific approaches. Examples include:

- Secure Shared Learning in Healthcare: Inference of Hospital Infection Risks
- Mobile Phone Data for Society and Privacy for the Individual: From the Conflict to a Synergy in Transport Flows Analysis
- A Novel Technology for Detecting Deceptive Behavior

Impact, Outreach and Policy

Cooperation is crucial for creating a safe cyberspace. The Blavatnik ICRC enjoys close relations with government, business and research partners and works together with both Israeli and foreign stakeholders to develop groundbreaking ideas.

The Eighth Annual Cyber Week 2018: Rapid Growth in Speakers and Partners

With over 8,000 participants from 80 countries, Cyber Week 2018 was our biggest conference yet. Comprised of over 50 events and welcoming over 400 speakers, Cyber Week was the biggest conference in the series. Cyber Week attracts the widest range of prominent speakers: C-Suite executives, government leaders, researchers and innovators, come together to discuss the most pressing issues in the cyber field today. Top governmental officials, scholars and executives from the US, UK, India, Singapore and Europe attended and addressed Cyber Week 2018.

Prime Minister Netanyahu Addressing The Cyber Week 2018 Main Plenary

Israeli Prime Minister Benjamin Netanyahu speaks at a cyber security conference held at Tel Aviv University, Israel June 26, 2017.
REUTERS/Amir Cohen

Prime Minister Netanyahu presented a short video at the Cyber Week 2018 Main Plenary. This photo was selected "Photo of the Year" by HaAretz daily.

See Appendix A & Appendix B for full **Cyber Week 2018** details

The Fourth Annual Ambassadors' Summit 2018

The annual Ambassadors' Summit is a dedicated event that exposes ambassadors and diplomats stationed in Israel to our expertise. This raises global awareness of our activities, develops the recognition of Blavatnik ICRC, and supports Israel's cyber strategy. The February 2018 Ambassadors' Summit focused on digital diplomacy.

Cyber Leaders Forum

We are bringing together a significant group of foreign officials from like-minded countries. The invitation-only closed event establishes our positive role in international cooperation.

THE WAY FORWARD

Blavatnik ICRC has already demonstrated considerable achievements in research and outreach alike. However, ever-evolving cyber technologies will evoke new challenges as well as opportunities. As much as our human and material resources allow, Blavatnik ICRC will sustain the strategic thrust to become one of the world's leading cyber research centers.

Sincerely,

Major Gen. (Ret.) Prof. Isaac Ben Israel
Director of the Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University
Isaac Ben Israel

GOVERNANCE AND MANAGEMENT

The Blavatnik ICRC is governed by the scientific and steering committees, advisory board and executive management. The management is comprised mostly of faculty and stakeholders, who perform these duties without compensation from the Blavatnik ICRC.

SCIENTIFIC COMMITTEE

The roles of the Scientific Committee are:

- Recommend scientific areas of focus in the Blavatnik ICRC
- Evaluate research proposals to the research fund, direct the scholarly peer review process, and recommend appropriate funding level
- Recommend activities and events the Blavatnik ICRC should host
- Suggest investments in research infrastructure
- Invite world-renowned scholars to Blavatnik ICRC

The Scientific Committee is composed of twelve senior TAU faculty members with extensive academic and scientific knowledge.

STEERING COMMITTEE

The Steering Committee's roles are:

- Approve work regulations.
- Approve the annual budget.
- Discuss Scientific Committee proposals regarding tasks, goals and annual assessments, research trials in the fund and their confirmation.
- Discuss focused activities, based on the recommendations of the Scientific Committee.
- Approve the selected research that was submitted to the research fund and received the recommendation of the Scientific Committee.
- Indicate the areas of engagement for each of the appointed ICRC researchers.
- Monitor the activity of the Blavatnik ICRC.

The decisions of the Steering Committee are made by a majority vote and are summarized in writing. The Steering Committee is composed of nine members: both TAU representatives and National Cyber Directorate representatives.

Barzilay, O., Geva, H., Goldstein, A., & Oestreicher-Singer, G. (2018). *Open to Everyone? The Long Tail of the Peer Economy: Evidence from Kickstarter*. Paper presented at the International Conference on Information Systems, San Francisco. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1045&context=icis2018

Bermanis, A., Wolf, G., & Averbuch, A. (2016). Diffusion-based kernel methods on Euclidean metric measure spaces. *Applied and Computational Harmonic Analysis, 41*(1), 190-213. http://dx.doi.org/10.1016/j.acha.2015.07.005

Birnhack, M. (2018). הדיגיטלית בעיר הפרטיות על הגנה. In T. Hatuka (Ed.), העיר הדיגיטלי בעידן (pp. 56-85). https://ssrn.com/abstract=32913832T

Birnhack, M., Toch, E., & Hadar, I. (2014). Privacy Mindset, Technological Mindset. *Jurimetrics, 55*(1), 55-114. http://www.jstor.org/stable/24395620

Carmon, E., Seifert, J.-P., & Wool, A. (2017, 1-5 May 2017). *Photonic side channel attacks against RSA*. The 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA. https://ieeexplore.ieee.org/abstract/document/7951801

Demchak, C. C., & Shavitt, Y. (2018). China's Maxim–Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking. *Military Cyber Affairs, 3*(1), 7. https://doi.org/10.5038/2378-0789.3.1.1050

Deutsch, L., & Horn, D. (2018). The Weight-Shape decomposition of density estimates: A framework for clustering and image analysis algorithms. *Pattern Recognition, 81*, 190-199. https://doi.org/10.1016/j.patcog.2018.03.034

Faisal, M., Cardenas, A. A., & Wool, A. (2016, 17-19/10/2016). *Modeling Modbus TCP for intrusion detection.* Paper presented at the Communications and Network Security (CNS), 2016 IEEE Conference, Philadelphia, PA.

Feder, A., Gandal, N., Hamrick, J. T., & Moore, T. (2017). The impact of DDoS and other security shocks on Bitcoin currency exchanges: evidence from Mt. Gox. *Journal of Cybersecurity, 3*(2), 137-144. https://doi.org/10.1093/cybsec/tyx012

Feibish, S. L., Afek, Y., Bremler-Barr, A., Cohen, E., & Shagam, M. (2017). *Mitigating DNS random subdomain DDoS attacks by distinct heavy hitters sketches.* Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies, San Jose, CA, USA. https://ieeexplore.ieee.org/abstract/document/7860524

Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics, 95*, 86-96. https://doi.org/10.1016/j.jmoneco.2017.12.004

Geva, H., Barzilay, O., & Oestreicher-Singer, G. (2017). *A Potato Salad with a Lemon Twist: Using Supply-Side Shocks to Study the Impact of Low- Quality Actors on Crowdfunding Platforms.* Paper presented at the 38th International Conference on Information Systems (ICIS). https://aisel.aisnet.org/icis2017/Peer-to-Peer/Presentations/3/

Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., & Balissa, A. (2018). Privacy by designers: software developers' privacy mindset. *Empirical Software Engineering, 23*(1), 259-289. https://doi.org/10.1007/s10664-017-9517-1

Harel, Y., Gal, I. B., & Elovici, Y. (2017). Cyber Security and the Role of Intelligent Systems in Addressing its Challenges. *ACM Transactions on Intelligent Systems and Technology (TIST), 8*(4), 1-12. https://doi.org/10.1145/3057729

Hatuka, T. (Ed.) (2018). העיר בעידן הדיגיטלי – תכנון, טכנולוגיה, פרטיות ואי־שוויון. אוניברסיטת תל אביב. http://bit.ly/2TJYeUE2T

Hatuka, T., Rosen-Zvi, I., Birnhack, M., Toch, E., & Zur, H. (2018). The Political Premises of Contemporary Urban Concepts: The Global City, the Sustainable City, the Resilient City, the Creative City, and the Smart City. *Planning Theory & Practice, 19*(2), 160-179. https://doi.org/10.1080/14649357.2018.1455216

Hirschprung, R., Toch, E., Schwartz-Chassidim, H., Mendel, T., & Maimon, O. (2017). Analyzing and Optimizing Access Control Choice Architectures in Online Social Networks. *ACM Transactions on Intelligent Systems and Technology (TIST), 8*(4), 1-22. https://doi.org/10.1145/3046676

Horn, D. (2018). Field Formulation of Parzen Data Analysis. *arXiv preprint arXiv:1808.08776*. https://arxiv.org/abs/1808.08776

Jarovsky, A., Milo, T., Novgorodov, S., & Tan, W.-C. (2018). *Rule sharing for fraud detection via adaptation.* Paper presented at the 2018 IEEE 34th International Conference on Data Engineering (ICDE).

Katz, O., Rinetzky, N., & Yahav, E. (2018). *Statistical Reconstruction of Class Hierarchies in Binaries.* Proceedings of the 23rd ACM International Conference on Architectural Support for Programming Languages and Operating Systems ASPLOS'18, Williamsburg, VA. https://ieeexplore.ieee.org/iel7/8476188/8509221/08509242.pdf

Khyzha, A., Attiya, H., Gotsman, A., & Rinetzky, N. (2018). *Safe Privatization in Transactional Memory*. Paper presented at the PPoPP Principles and Practice of Parallel Programming 2018: 23rd ACM Special Interest Group on Programming Languages (SIGPLAN) Annual Symposium on Principles and Practice of Parallel Programming, Vösendorf / Wien, Austria. https://dl.acm.org/citation.cfm?id=3178487

Kleinmann, A., & Wool, A. (2015). *A statechart-based anomaly detection model for multi-threaded SCADA systems.* Paper presented at the International Conference on Critical Information Infrastructures Security. https://link.springer.com/chapter/10.1007/978-3-319-33331-1_11

Kleinmann, A., & Wool, A. (2016). *Automatic construction of statechart- based anomaly detection models for multi-threaded SCADA via spectral analysis.* Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy. https://dl.acm.org/citation.cfm?id=2994490

Kleinmann, A., & Wool, A. (2017). Automatic Construction of Statechart- Based Anomaly Detection Models for Multi-Threaded Industrial Control Systems. *ACM Transactions on Intelligent Systems and Technology (TIST), 8*(4), 1-21. https://doi.org/10.1145/3011018

Levin, A. (2018). Privacy by Design by Regulation: The Case Study of Ontario. *Canadian Journal of Comparative and Contemporary Law, 4*, 115. http://www.cjccl.ca/wp-content/uploads/2018/08/Levin-Privacy-by-Design- by-Regulation.pdf

Levy, D., & Wolf, L. (2017). *Learning to Align the Source Code to the Compiled Object Code*. Paper presented at the Proceedings of the 34th International Conference on Machine Learning, Proceedings of Machine Learning Research. http://proceedings.mlr.press

Lupovici, A. (2014). The Attribution Problem and the Social Construction of Violence: Taking Cyber Deterrence Literature a Step Forward. *International Studies Perspectives* 17(3), https://doi.org/10.1111/insp.12082

Lupovici, A. (2018). Toward a Securitization Theory of Deterrence. *International Studies Quarterly*, https://doi.org/10.1093/isq/sqy045

Maltinsky, A., Giladi, R., & Shavitt, Y. (2017). On Network Neutrality Measurements. *ACM Transactions on Intelligent Systems and Technology (TIST), 8*(4), 1-22. https://doi.org/10.1145/3040966

Meyer, J. (2017). Evaluating alerting systems from descriptions. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 61*(1), 307-307. https://doi.org/10.1177/1541931213601557

Milo, T., Novgorodov, S., & Tan, W.-C. (2016). Rudolf: interactive rule refinement system for fraud detection. *Proceedings of the Very Large Database Endowment, 9*(13), 1465-1468. https://doi.org/10.14778/3007263.3007285

Mukherjee, S., Padon, O., Shoham, S., D'Souza, D., & Rinetzky, N. (2017). *Thread-local semantics and its efficient sequential abstractions for race-free programs.* Paper presented at the 24th International Static Analysis Symposium. http://dx.doi.org/10.1007/978-3-319-66706-5_13

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. *Foresight*. https://doi.org/10.1108/FS-02-2018- 0020

Schuster, R., Shmatikov, V., & Tromer, E. (2017). *Beauty and the burst: Remote identification of encrypted video streams.* Paper presented at the USENIX Security. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17- schuster.pdf

Tabansky, L. (2016). *Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy.* Paper presented at the 8th International Conference on Cyber Conflict (CyCon16), Tallinn, Estonia. https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2004%20Towards%20a%20Theory%20of%20Cyber%20Power%20-%20the%20Israeli%20Experience%20with%20Innovation%20and%20Strat egy.pdf

Tabansky, L. (2017). Cybered Influence Operations: towards a scientific research agenda. *Security Policy Library – The Norwegian Atlantic Comittee, 2017*(2), 36. http://www.atlanterhavskomiteen.no/nettsider/dnak/publikasjoner/sikkerhets politisk-bibliotek

Tabansky, L. (2018). Sticking to their Guns: The Missing RMA for Cybersecurity. *Military Cyber Affairs, 3*(2), 23. https://doi.org/https://doi.org/10.5038/2378-0789.3.1.1039

Tabansky, L., & Ben-Israel, I. (2015). *Cybersecurity in Israel*: Springer.

Trabish, D., Mattavelli, A., Rinetzky, N., & Cadar, C. (2018). *Chopped Symbolic Execution.* Paper presented at the ICSE 2018 https://www.icse2018.org/event/icse-2018-technical-papers-chopped- symbolic-execution

Tzezana, R. (2016). Scenarios for crime and terrorist attacks using the internet of things. *European Journal of Futures Research, 4*(1), 18. https://doi.org/10.1007/s40309-016-0107-z

Tzezana, R. (2017). High-probability and wild-card scenarios for future crimes and terror attacks using the Internet of Things. *Foresight, 19*(1), 1- 14. https://doi.org/10.1108/FS-11-2016-0056

Zilberman, N., & Shavitt, Y. (2016). Setting the Foundations for PoP-Based Internet Evolution Models. *arXiv preprint arXiv:1612.04096*. http://arxiv.org/abs/1612.04096v2

Zrahia, A. (2018). Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views. *Journal of Cybersecurity, 4*(1). https://doi.org/10.1093/cybsec/tyy008

כהן, דניאל, and 64-69 .(2018)מערכות "שימוש בלוחמת סייבר למבצעי השפעה צבאיים." גיל ברעם. no. 480-481,

EIGHTEEN NEW RESEARCH GRANTS AWARDED IN 2018

Blavatnik ICRC has now funded seventy-four research projects.

We published The Blavatnik Interdisciplinary Cyber Research Center Call for Research Proposals, 2018 in Q1 2018 (See Appendix C). The Call for Research Proposals was distributed throughout Israeli academia, our partners and researcher's networks.

FUNDING DECISIONS PROCESS: SCHOLARLY PEER REVIEW AND STEERING COMMITTEE

At the first stage in the scholarly peer review process, the Scientific Committee members read the submitted proposals. Each member hands in remarks and recommendations confidentially to the Scientific Committee chair.

A subsequent Scientific Committee meeting serves to discuss, debate, and make editorial decisions. The Scientific Committee then selects the research proposals that cleared the first stage of the review.

The Scientific Committee sends the research proposals to external referees for expert peer-review.

The Scientific Committee may request the PIs for additional clarifications needed on proposals, it will request the PIs for this information.

A subsequent Scientific Committee is dedicated to discuss refereed proposals and make funding decisions.

After reviewing the submitted proposals and their funding requests, the Scientific Committee solicits a funding recommendation to the Steering Committee for final approval. The Steering Committee also asserts the relevance of the research to cyber.

Conflict of Interest Prevention

A committee member will not participate in the review process of any proposal in which he/she or one of his/her current or former students are directly involved financially.

The same will hold in respect to any proposal where the committee member claims a conflict of interest for whatever reason.

Thirty-one valid submissions received from various disciplines went through two rounds of reviews and revisions. Following the Steering Committee decisions and two Steering Committee meetings, we awarded research grants to eighteen of the thirty-one submissions.

Blavatnik ICRC Research Grants Awarded in 2018

Title	PI 1 Name	PI1 TAU affiliation	PI 2 Name	PI 2 affiliation
The Viciousness and Caring of Sharing: Conflicts and Motivations of Online Shamers	Yael Steinhart	Coller School of Management Department of Marketing	Chen Pundak	PhD Candidate, Coller School of Management
Detecting Cryptocurrency Scams and Measuring Cryptocurrency Quality	Neil Gandal	Eitan Berglass School of Economics	Marie Vasek	Professor of Computer Science, University of New Mexico
The Dynamics and Geography of the Cybersecurity Industry	Tali Hatuka	Geography and the Human Environment Lester and Sally Entin Faculty of Humanities	Erran Carmel	American University, Kogod School of Business

Title	PI 1 Name	PI1 TAU affiliation	PI 2 Name	PI 2 affiliation
Righting Our Wrongs in Digital Downloading: The Mutual Influence of Legal Consequences and Social Norms on Willingness to Engage in Moral Regulation	Yael Steinhart	Coller School of Management	Ayelet Gneezy	Professor, Rady School of Management University of California, San Diego
The Implications of the GDPR on Higher Education System in the Era of Digital Education	Tal Soffer	Jaime and Joan Constantiner School of Education, Lester and Sally Entin Faculty of Humanities	Anat Cohen	Jaime and Joan Constantiner School of Education, Lester and Sally Entin Faculty of Humanities
Mobile Phone Data for Society and Privacy for the Individual: From the Conflict to a Synergy in Transport Flows Analysis	Itzhak Benenson	Department of Geography and Human Environment, School of Geosciences, Raymond and Beverly Sackler Faculty of Exact Sciences	Itzhak Omer	Department of Geography and Human Environment, School of Geosciences, Raymond and Beverly Sackler Faculty of Exact Sciences
Non-Public Hacks	Roy Zuckerman	Coller School of Management		
A Novel Technology for Detecting Deceptive Behavior	Dino Levy	Coller School of Management and Sagol School of Neuroscience	Yael Hanein	Prof. of Electrical Engineering, Director, TAU Center for Nanoscience and Nanotechnology (2012 – present)
The Blame Game: National Strategies During Cyber Conflict	Udi Sommer	Department of Political Science, Gershon H. Gordon Faculty of Social Sciences	Gil Baram	PhD Candidate Department of Political Science, Gershon H. Gordon Faculty of Social Sciences
Towards Higher Accuracy of Behavioral Big Data Analysis: Using Qualitatively Augmented Hierarchical Classifier Algorithms	Dov Te'eni	Coller School of Management	David G. Schwartz	Information Systems, Grad. School of Business Administration, Bar Ilan University
Security Hardening against Hardware Vulnerabilities through Hardware Separation	Erez Shmueli	Department of Industrial Engineering, Iby and Aladar Fleischman Faculty of Engineering	Assaf Schuster	Department of Computer Science, Technion

Title	PI 1 Name	PI1 TAU affiliation	PI 2 Name	PI 2 affiliation
Competition and Incentives for Information Exchange Regarding Cyber Security Threats	Noam Shamir	Coller School of Management	Hyoduk Shin	Rady School of Management UC San Diego
Memory Access Safety-Checking Tools for Programs that Share Memory with Devices	Adam Morrison	Blavatnik School of Computer Science	Dan Tsafrir	Department of Computer Science, Technion
The Deterrence Strategies of Non- States Cyber Actors	Amir Lupovici	Department of Political Science, Gershon H. Gordon Faculty of Social Sciences		
Secure Shared Learning in Healthcare: Inference of Hospital Infection Risks	Benny Chor	Blavatnik School of Computer Science	Galia Rahav	Sackler Faculty of Medicine, Sheba Medical Center
Automatically Verifying User Kernel Extensions	Mooly Sagiv	Blavatnik School of Computer Science	Noam Rinetzky	Blavatnik School of Computer Science
Future Crimes Enabled by Blockchain-Based Technologies	Roey Tzezana	Research fellow, Humanity Centered Robotic Initiative (HCRI), Brown University, USA		
Values and Cyber Security	Neil Gandal	Berglas School of Economics	Sonia Roccas	The Open University of Israel, Professor of Psychology

Most of the research plans are for 24 months.

Automatically Verifying User Kernel Extensions

Prof. Mooly Sagiv, Prof. Noam Rinetzky, Dr. Aurojit Panda

Symbolic techniques for reasoning about programs have drastically advanced in the last three decades. We propose to develop novel techniques for harnessing symbolic techniques for proving the safety of dynamically loaded user-programs extending operating system kernels, thus ensuring that the integrity of the operating system is preserved.

The main challenge we face is mitigating the complexity of the verification process. Therefore, we propose to split the process into two parts: (i) a complex off-line verifier that generates proofs of integrity and (ii) a simple in-kernel proof-checkers that validates the correctness of a program annotated with an existing proof. The first phase is executed at compile-time in user mode, and thus the complex verifier does not need to be trusted. The second phase is executed at load-time in kernel mode by a simple trusted checker.

Secure Shared Learning in Healthcare: Inference of Hospital Infection Risks

Prof. Galia Rahav, Prof. Benny Chor, Dr. Adi Akavia, Prof. Zohar Yakhini

The use of data science to support inference in medical science has seen great progress in recent years and is a very active research domain with important practical implications. The application of state-of-the-art

techniques in this context requires skill and knowledge as well as large volumes of data, to support higher confidence statistics. Single health providers, such as hospitals, can often access limited data volumes and can benefit from sharing data with other providers. Moreover, health providers are not focused on the machine learning and statistical aspects of the project, and can benefit from outsourcing learning tasks to a third party. Both of the above aspects of health related leaning and inference projects, sharing and outsourcing, pose security risks.

We propose to develop methods, algorithms and protocols to enable secure data sharing for performing machine learning tasks on data combined from several parties. The protocols will support the sharing and transfer of encrypted or masked data; the performance of learning on said protected data, with no significant leakage of information; and the secure communication of the learning results to the data providers.

As example use cases, to support our protocol development and optimization, we will address the use of sparse linear regression and logistic regression to predict risk of infection in hospitals.

Deterrence Strategies of Non-States Cyber Actors

Dr. Amir Lupovici

The main research questions are:

1. Which non-state actors employ cyber deterrence strategies, and how do they do so?
2. What conditions impact the effectiveness of cyber deterrence strategies employed by these non-state actors?

More specifically, this project aims to map the different non-state actors that employ cyber deterrence strategy based on the type of cyber actor (the defender) and the type of challenger (e.g., state/non-state actors). I will further map these practices by categorizing the various ways these actors attempt to employ cyber deterrence strategy, as well as the undesired behaviors the strategy aims to dissuade. My analysis will not only elaborate on deterrence strategies already acknowledged in deterrence scholarship—that is, deterrence by punishment and by denial—but will also develop a relatively new concept—deterrence by detection.

Focusing on how non-state actors are involved in practices of deterrence further demonstrates the importance of these actors in international politics, and even in security practices. This involves reconceptualizing what security is and whom it is for (Buzan et al., 1998; Wyn Jones, 1999: 93-124). Among other things, it also allows us to recognize and explore how new "superpowers" in world politics adopt and adapt traditional security practices. Furthermore, it explores how these actors try to transform their potential power into actual power and influence other (international) actors.

Rethinking what security is in the context of non-state cyber actors also points to another important issue: that is, the security of individuals. The growing importance of non-state cyber actors in world politics increases the general global population's reliance on these actors, affecting individuals' security, safety, and privacy. Non-state cyber actors' growing acknowledgement and awareness of the liability and need to protect individuals (and their data) may increase the use of cyber deterrence practices. Nonetheless, these practices might also, in some cases, conflict with people's security.

Memory Access Safety-Checking Tools for Programs that Share Memory With Devices

Dr. Adam Morrison, Dr. Dan Tsafrir

Memory access vulnerabilities (such as buffer overflow) are prevalent in unmanaged programming languages, and concurrent memory access vulnerabilities are prevalent in managed and unmanaged languages alike. Significant research has therefore been

put into developing tools that help programmers identify and protect against such vulnerabilities. We observe, however, that (1) setups allowing programs to utilize non- CPU devices that independently access the memory are becoming increasingly popular, and that (2) none of the aforementioned tools are applicable in such setups. We propose to investigate this problem and make the first step towards a solution.

Competition and Incentives for Information Exchange Regarding Cyber Security Threats

Dr. Noam Shamir, Dr. Hyoduk Shin

In this research proposal we examine in a rigorous manner a few important aspects of the legislation to counter cyber-security threats by sharing information regarding potential cyber-attacks. We first evaluate the claim that a shared database of security- threats benefits the private sector. Second, and more importantly, we evaluate the incentives of a company, operating in a competitive market, to contribute its information regarding cyber-security threats. In this work we highlight a few effects that a company must take into consideration when it reveals information regarding cyber-security threats. Gaining information about cyber-security threats, which other companies in the industry faced, allows the company to better protect its strategic IT assets – an effect that benefits a company. However, at the same time, revealing information about its own vulnerabilities can hinder the ability of the company to compete in an efficient manner in the market place. We analyze this trade-off, and examine under which conditions companies will choose in a voluntarily manner to share cyber-security information.

Security Hardening Against Hardware Vulnerabilities Through Hardware Separation

Dr. Erez Shmueli, Prof. Assaf Schuster, Dr. Nadav Amit

The recently discovered security vulnerabilities that exploit micro-architectural properties introduce new challenging attack vectors. Adapted mitigation techniques address the discovered vulnerabilities, but might not prevent other yet unknown ones. Moreover, the overheads of existing mitigation techniques are high and may deter users from enabling them. Current protection schemes against these vulnerabilities are rather complicated, and consist of an extensive operating system (OS) changes and new microcode features. Due to this scheme complexity, the protection from these vulnerabilities might be incomplete. Furthermore, it is yet unclear whether future CPU enhancements will render the current complicated protection scheme unnecessary.

In our research, we wish to explore the solution space for the mitigation against this new class of security vulnerabilities, including yet undiscovered ones, and to study the inherent trade-off between protection and performance. To protect against these vulnerabilities, we wish to take a more drastic measure, by separating the hardware resources, computer, and memory, which are allocated to the OS and its processes. This separation can be done in different levels to serve diverse purposes: weak separation to

complement current protection schemes by alleviating their overheads, and strong separation to protect against unknown security threats.

A Novel Technology for Detecting Deceptive Behavior

Dr. Dino Levy, Prof. Yael Hanein

How can we prevent attempts of deception? This question has paramount importance for a wide array of fields, ranging from everyday social interactions, to finance (e.g., protection against fraud), business (e.g., gauging negotiator's credibility), and security (e.g., in border protection). In the context of cyber-security, millions of people perform online interactions every day. It is extremely difficult for cyber-security professionals to decide whether the individual is being forthright or deceptive. The limitation of human vigilance and perception renders them unable to reliably detect deceit, with performance around chance for novices. A meta-analysis of 206 studies, all asking subjects to judge deception based on a brief encounter with an unfamiliar partner in real time, reports an average of 47% correct identification of lies and 61% of truths. This performance is just slightly higher for experts, such as law enforcement personnel.

The goal of the proposed research is to develop and test a novel autonomous system to detect deception in videos, based on the integration of unique physiological recordings and machine learning algorithms. This approach has direct online applications in ticket purchases, online meetings, job interviews, loan applications, and other situations where online deceptive communication might appear and security is important.

Non-Public Hacks

Dr. Roy Zuckerman

In this study, we investigate the preponderance of obtaining non-public financial information through cyber hacks. Using data acquired from a major networking equipment provider, we find that attempted hacks on public companies' HQs rise by up to 60% during the 14 calendar days preceding the release of quarterly earnings. Attacks drop to normal levels a day after the earnings release. We find no such effect for private companies in our dataset. The results remain robust after controlling for day of the week, malware activity and other seasonal effects. We find no significant abnormal returns for the firms in our sample prior to the release of quarterly earnings. Taken together, these results imply that cyber hackers have significant interest in obtaining non-public financial information prior to its release.

Mobile Phone Data for Society and Privacy for the Individual: From the Conflict to a Synergy in Transport Flows Analysis

Prof. Itzhak Benenson, Prof. Itzhak Omer, Raazesh Sainudiin

Smart cities demand sound knowledge on citizens' presence and mobility. Mobile phone data is the source of such knowledge. Based on cellular data, urban population and its mobility, it can be mapped to spatial resolution of tens of meters and temporal resolution of minutes, and the precision will soon rise to meters and seconds. However, increasing quality and precision of location data comes at the expense of an unprecedented drop in personal privacy. Cellular data suppliers clearly understand this danger and are stalled in a controversial tradeoff. As a result, practical implementation of a vast spectrum of smart city ideas is delayed again and again.

Transportation and urban science define demands and impose essential limitations concerning, the level of aggregation of cellular data. For example, to establish a new bus stop or add a dedicated bus

lane to the existing road, the locations and routes of urban travelers should be known at high spatial and temporal resolutions. The maps of transportation flows, by modes (private cars, public transport, bikers, pedestrians), translated into spatially extended graphs, are the major information component for the modern methods of transportation planning and management. Systematic reassessment of urban traffic flows is cornerstone of the future smart city that will evolve with respect to evolving citizens' demands.

Privacy vulnerabilities are inherent for the location-based data and hiding personal identifiers (e.g., by replacing them with pseudonyms) is insufficient to guarantee anonymity since the location could still lead to the identification of the individual. Relevant security and decision-theoretic methods are thus needed for the anonymization of individual location-based queries in order to preserve privacy when extracting value for the society from locational data.

Our research aims at establishing the necessary and sufficient space-time resolution and level of aggregation of mobility data that are required for the smart city transportation planning and management and, at the same time, clearly understand the potential harms to privacy, avoid disclosure of individual information and establish the forms of mobility data supply and procedures of data management and analysis in order to guarantee individual privacy. The outcome of this interaction should be clear privacy-preserving rules of mobility data aggregation for transportation planning and management.

To achieve this goal, we will:

Develop privacy-preserving mathematical models for the dynamics of co-trajectories using clustering methods and continuous-time Markov chains;

Train the model with data from millions of transformed individual trajectories over several months using latest distributed fault-tolerant big-data algorithms;

Quantify the effect of privacy, specified through the spatial resolution of individual trajectories, and on the statistical risk of the model's parameter estimates with respect to the requirements of transportation planning and management.

The empirical research will be conducted in a selected area of the Tel Aviv metropolitan region.

Implications of the Gdpr on the Higher Education System in the Era of Digital Education

Dr. Tal Soffer; Dr. Anat Cohen; Dr. Yoel Raban

The General Data Protection Regulation (GDPR) of the European Union aims to strengthen data protection for individuals mainly by allowing them to have more control over their personal data. One of the sectors the GDPR will impact on is the education sector in general, and higher education in particular. Most higher education institutions make extensive use of emerging technologies (e.g. LMS: Learning Management Systems), in teaching and learning processes. On the one hand, LMS usage enables the improvement of learning and instruction. It also may provide insights into educational practices, through analyzing the retrieved ('mined') log data, using learning analytics (Davis et al., 2017). On the other hand, they may intrude on the privacy of students and teachers, and create ethical problems. In the light of the new GDPR, we should find the appropriate balance between improving learning and instruction and data protection and privacy. Therefore, there is a need to raise awareness among all stakeholders in the institute about the relevant privacy issues and their digital literacy, as well as integrate clear explanation on privacy and data protection policies (Farah et al., 2017).

There are limited studies regarding the impact of the GDPR on the educational system in general and on higher education in particular. Specifically, studies that explore the issue from a wider and holistic

perspective, taking into consideration all the main stakeholders (institutional decision makers, teachers, students and technological developers) and propose clear comprehensive understanding of the pedagogical challenges, along with the GDPR, and propose inclusive policy. Thus, the main goals of the study are:

a) to describe the need for transforming higher education under the regime of the new GDPR in light of the growing usage of emerging technologies.

b) to recommend a policy for performing the necessary changes to comply with these regulations, taking into consideration the potential pedagogical aspects stemming from the usage of emerging technologies.

The exploratory study will be conducted at TAU, using a mix method methodology, combining qualitative and quantitative data by means of triangulation. In order to gather as much data as possible about the impact of the GDPR on higher education, several information sources were singled out: literature reviews and institutional statistical data, semi-structured interviews with relevant stakeholders, surveys with teachers and students and a brainstorming workshop.

Based on the results of this study, a compliant policy for educational institutions will be formulated, taking into consideration the needs of all various stakeholders (institutional decision makers, teachers, students and technological developers) in different aspects such as: educational (training), technological (privacy by design), legal (regulations) etc.

Viciousness and Caring of Sharing: Conflicts and Motivations of Online Shamers

Dr. Dikla Perez, Dr. Ayelet Gneezy, Prof. Yael Steinhart and Shirly Bluvstein

Despite all of the technological advances, cyber-security is to a large extent determined by the behavior of the end-users. The integrity the network depends on is the willingness of the users to adhere to security guidelines. Increasing awareness to security threats and the steps that should be taken to avoid them is an important factor. However, increased awareness is not sufficient to ensure safe behavior. People often behave in ways that expose them to the risk of undesirable consequences even when they are well aware of these consequences (unhealthy eating habits, unsafe driving practices, etc.). Thus, a different approach is needed to identify factors that increase willingness of end-users to adopt safe behavior.

We will apply the vast knowledge accrued on personal values for this purpose. Personal values are cognitive representations of abstract, desirable motivational goals that guide the way individuals select actions, evaluate people and events, and explain their actions and evaluations. They are a core aspect of people's identity, and serve as standards or criteria that provide social justification for choices and behaviors across situations. Values are recognized as important psychological constructs, because, as guiding principles in people's lives, they are hypothesized to have wide- ranging effects. Lately, the effects of personal values on preferences, choices and behaviors have evoked much interest.

Behavior that is inconsistent with cyber-security is usually not malicious, and not random. It serves to attain important motivations. Informing users that a specific practice is unsafe is only useful to the extent to which the primary motivation of the users is to obtain safety. But safety is rarely the core motivations of end-users.

A first step in a program of research aimed at changing behavior of end users is to identify the values that are associated with behavior that breaches security: For example, sharing intimate information is consistent with social connectedness (the motivation captured by self-transcendence values), sharing information about one's success is consistent with self enhancement values.

To examine whether user values affect network security, we will conduct empirical studies in laboratory settings. Participants will be 300 University students and staff. Participants will first answer the "Schwartz

values" questionnaire. This will enable us to have quantitative measures for the importance of each value. In this survey, we will also measure relevant personality traits (impulsivity) and computer experience.

We will then expose users to several computerized "in basket" email tasks. Some of the emails will be legitimate, while some will be phishing attempts. Participants will be instructed that they will need to distinguish between legitimate emails (whose content needs to be addressed), spam emails (which can be deleted) and phishing attempts (which should be put in a separate folder). They will be compensated according to their accuracy, thus creating an incentive to correctly identify each type of message. We will give the users a relatively full 'inbox,' in order to simulate the real world in which employees often must rapidly deal with a large number of emails. In order to simulate time pressures, some participants will have a time limit to complete the tasks, while others will not have a time limit. Users will randomly be assigned to one of the two categories.

Some of the phishing attempts will be specifically related to different values, e.g. seeking help -- is related to altruistic values. The order of the email tasks will be randomized across participants. It may be that people with different values fall prey to specific types of phishing attempts, or it may be that people with certain types of values (perhaps altruistic ones) are more likely to fall prey in general to phishing attempts. Our empirical work will be able to examine both of these hypotheses.

Values and Cyber Security

Prof. Neil Gandal, Prof. Sonia Roccas

Despite all of the technological advances, cyber-security is largely determined by the behavior of the end-users. The integrity the network depends on is the willingness of the users to adhere to security guidelines. Increasing awareness to security threats and the steps that should be taken to avoid them is an important factor. However, increased awareness is not sufficient to ensure safe behavior. People often behave in ways that expose them to the risk of undesirable consequences even when they are well aware of these consequences (unhealthy eating habits, unsafe driving practices, etc.). Thus, a different approach is needed to identify factors that increase willingness of end-users to adopt safe behavior.

We will apply the vast knowledge accrued on personal values for this purpose. Personal values are cognitive representations of abstract, desirable motivational goals that guide the way individuals select actions, evaluate people and events, and explain their actions and evaluations. They are a core aspect of people's identity, and serve as standards or criteria that provide social justification for choices and behaviors across situations. Values are recognized as important psychological constructs, because, as guiding principles in people's lives, they are hypothesized to have wide-ranging effects. Lately, the effects of personal values on preferences, choices and behaviors have evoked much interest.

Behavior that is inconsistent with cyber-security is usually not malicious, and not random. It serves to attain important motivations. Informing users that a specific practice is unsafe, is only useful to the extent to which the primary motivation of the users is to obtain safety. But safety is rarely the core motivation of end-users.

A first step in a program of research aimed at changing behavior of end users is to identify the values that are associated with behavior that breaches security: For example, sharing intimate information is consistent with social connectedness (the motivation captured by self-transcendence values), sharing information about one's success is consistent with to self enhancement values.

To examine whether user values affect network security, we will conduct empirical studies in laboratory settings. Participants will be 300 University students and staff. Participants will first answer the "Schwartz

values" questionnaire. This will enable us to have quantitative measures for the importance of each value. In this survey, we will also measure relevant personality traits (impulsivity) and computer experience.

We will then expose users to several computerized "in basket" email tasks. Some of the emails will be legitimate, while some will be phishing attempts. Participants will be instructed that they will need to distinguish between legitimate emails (whose content needs to be addressed), spam emails (which can be deleted) and phishing attempts (which should be put in a separate folder). They will be compensated according to their accuracy, thus creating an incentive to correctly identify each type of message. We will give the users a relatively full 'inbox,' in order to simulate the real world in which employees often must rapidly deal with a large number of emails. In order to simulate time pressures, some participants will have a time limit to complete the tasks, while others will not have a time limit. Users will randomly be assigned to one of the two categories.

Some of the phishing attempts will be specifically related to different values, e.g. seeking help -- is related to altruistic values. The order of the email tasks will be randomized across participants. It may be that people with different values fall prey to specific types of phishing attempts, or it may be that people with certain types of values (perhaps altruistic ones) are more likely to fall prey in general to phishing attempts. Our empirical work will be able to examine both of these hypotheses.

The Blame Game: National Strategies During Cyber Conflict

Dr. Udi Sommer, Gil Baram

Cyber technology enables countries to act covertly: the results of offensive actions in the cyber realm and their influences are not always revealed to the public eye. Likewise, identifying who is behind a given attack may be complicated. Even if the upshots of the attack are publicly observable—e.g., damage to a power grid leading to the severance of electricity in an entire country—the attacked country can still dismiss these effects, arguing that they were the result of some technical failure rather than proof of a successful hostile action against it. Furthermore, any suspected attacker could use denial as a strategy. To date, however, our understanding of those strategies—both attacker and attacked—is limited theoretically and empirically.

Recent work regarding covert actions offers three mechanisms that induce credibility to signals of resolve in the covert sphere. These can make the use of covert actions even more appealing. First are sunk costs, which refer to situations when states decide to take covert action because of non-recoverable resources. Choosing covert action, leaders employ a more "creative" way of addressing security threats. Second are counter-escalation risks. Covert actions can signal resolve since they appear credible because of the risk of crisis escalation; leaders using covert signaling tools can be free to engage in more aggressive behavior. Last are domestic risks. Covert actions enable leaders to act more freely without risking the loss of public support. Those mechanisms suggest that countries will opt for covert actions to achieve political goals.

Accordingly, a key question arises: what causes countries—victims and attackers alike—to abandon the covert playing field for the public international arena when conducting their cyber feuds? Why would a country that was attacked choose to admit being harmed publicly, and why would an accused attacker choose to publicly admit or deny allegations? Why not simply remain silent and maintain ambiguity? Existing literature does not provide satisfying answers to any of these questions.

We propose to undertake the first comprehensive study to examine factors underlying the strategic choices of states involved in cyber conflicts. Choice of any specific strategy may have important implications for the country, its leaders, and its relations with other international actors. Therefore, it is necessary to examine

in depth the considerations that may influence national decision makers in choosing their strategy, the factors that lead to this choice and its implications.

At the center stands a novel theoretical framework we develop, which elucidates the variation in states' strategy and sheds new light on the broader topic of actors' decision-making process in cyberspace. This framework consists of an analysis of states' wide-ranging strategic, diplomatic and political considerations and their motivations to choose each strategy. We focus primarily on what leads states to forsake the benefits of anonymity and ambiguity by moving cyber conflict into the public sphere. Next, we examine the validity of our framework by analyzing empirical data, we originally collected and compiled, concerning interstate cyber conflict.

The research will be composed of three main parts. First, the theoretical model explains why countries choose to leave the covert sphere and go public. As a part of this section, we also analyze in depth the relative advantages and disadvantages of each of the possible strategies available for victims and (suspected) attackers. Second, we collect the necessary data to compile an updated cyber-attacks dataset. This component of the project constitutes its core. The analysis will be conducted in the third part in order to identify the circumstances and conditions under which states are more likely to choose to reveal the attack and to discover the relative influence of each type of consideration. We expect our results to shed new light on the conundrum that we observe empirically: how come states move away from the obscurity of the cyber arena and make cyber-attacks public?

Towards Higher Accuracy of Behavioral Big Data Analysis

Prof. Dov Te'eni, Prof. David G. Schwartz, Dr. Inbal Yahav

This interdisciplinary study develops a hybrid classification method that integrates qualitative analysis with classifier design for text and image analysis of online behavioral big data, which we call Qualitatively Augmented Text Classifier Algorithms (QATCA). This method will be developed and evaluated on an existing cyber intelligence platform that analyzes Dark Web activity undetectably and autonomously. The application of the method relies on computer support that not only aids qualitative

analysis and classifier design but also ensures the integration of both components. Efficient and effective classification of online behavioral big data is an important tool for cybersecurity. The output of this study will contribute to the analytical techniques addressing (1) cyber conflict and warfare issues (e.g., monitoring of cyber-crime and cyber-terror activities and the potential criminal's and terrorist's behavior); (2) security mechanisms, methodologies, and strategies (e.g., monitoring of online information leakages); and (3) online social networks and subversive behavior (e.g., automatic sentiment trend analysis).

Righting Our Wrongs in Digital Downloading

Dr. Dikla Perez, Dr. Ayelet Gneezy, Prof. Yael Steinhart and Shirly Bluvstein

Approximately 40% of digital content worldwide is downloaded illegally using the cyber space. Such illegal downloading not only threatens firms' motivation to invest in innovative digital content, but also costs the digital content industry over $4.6 billion per annum (IDC; Business Software Alliance 2015, International Federation of the Phonographic Industry (IFPI)(http://www.ifpi.org, Chien, Hsin & Lee, 2005). Of importance, these illegal actions have penetrated the social and legal aspects of individuals and firms. The sheer volume of piracy in cyberspace (which involves stealing intangibles such as software, movies, or games) suggests that such behaviors have become an accepted norm. Interestingly, these normative beliefs might be uniquely relevant to cyberspace, as outside of the cyberspace, accessing the property of others and using someone else's assets is a non-accepted norm. Therefore, a comprehensive

investigation of piracy in the cyber scape also requires attention to the normative beliefs that affect cyber pirates' behavior in cyberspace.

This research addresses the popularity of this illegal and unethical behavior in the cyber space and examines the conditions under which people decide to "right their wrongs" by agreeing to offer monetary compensation to content producers after engaging in illegal digital downloading. Specifically, we aim to examine whether (a) perceived social norms, (b) legal consequences, and (c) the interaction between them affect individuals' moral perceptions regarding illegal digital downloading and their consequent tendency to engage in moral regulation after downloading content illegally. Our experiments rely on an innovative paradigm for evaluating moral-regulation behavior, namely, offering individuals an opportunity to financially compensate (or express intentions to compensate) the party they have wronged.

Results of two preliminary studies suggest that participants are willing to retroactively pay for content that they previously downloaded illegally and that this tendency is affected by their perceptions of the social norms and legal consequences associated with illegal downloading, in addition to the perceived morality of such behavior. In the first study participants shared an actual incident in which they had downloaded content illegally (n=150, 46.8% males); 61.3% (n = 92) reported that they had downloaded a movie from a torrent site (e.g., Torrentz, Extratorrent or Kickasstorrent). Of the participants who had illegally downloaded a movie, 43% reported that they had done so within the last year. Moreover, 82.3% of participants reported that half or more of their friends and family members downloaded movies through torrent sites, and think that it is OK to do so. These findings suggest that participants perceived illegal digital downloads as being highly socially acceptable. Furthermore, 83.4% reported that they did not perceive any legal consequences to this act. Next, we measured participants' tendency to engage in moral regulation by offering them the opportunity to pay money to the original producer of the content they had reported downloading. Results show that 79% of participants agreed to hypothetically pay the producer some amount of money.

In the second study we manipulated participants' perceptions of the social norms and legal consequences associated with illegal downloads. We randomly assigned participants (n=166, 35.5% males) to four experimental conditions and measured their tendency to engage in moral regulation after hypothetically engaging in illegal digital downloading. We found that the perceived social acceptability of illegal downloads had a negative effect on tendency to engage in moral regulation; this effect was moderated by the perceived extent of legal consequences. Specifically, the effect was significant for the mild-legal-consequences condition (95% CI: -1.878 to -.274) and non-significant for the severe-legal-consequences condition (95% CI: -.829 to .775). Finally, we found that, in the mild-legal-consequences condition, moral perceptions of illegal digital downloading mediated the effect of social norms on tendency to engage in moral regulation (95% CI: -.679 to -.006); no such mediation effect was observed in the severe-legal-consequences condition (95% CI: -.093 to .476).

Dynamics and Geography of the Cybersecurity Industry

Dr. Tali Hatuka, Prof. Erran Carmel

Cybersecurity is now a global industry and has solidified three of its largest geographic ecosystems in Israel, Silicon Valley/San Francisco, and metropolitan Washington D.C. Understanding regional ecosystems (clusters) as areas of innovation emerged in the 1990s when Harvard's Michael Porter popularized the concept and Silicon Valley began to be celebrated. All firms in the cluster benefit from being near sources of information, to human capital, to venture capital, and to key buyers. The three cybersecurity clusters each have hundreds of firms in cybersecurity products and services. Using the Cybersecurity500 as a proxy of influence --24% of the important firms are in Silicon Valley, 10% are in Washington, and 8% are in Israel.

We are not aware of any academic studies that have taken an in-depth look at the cybersecurity industry nor at its major clusters. Thus, this study will be a first. Our research goals are: First, to assess and analyze the emergence and development of the cybersecurity industry, how this industry developed, where, and why it looks as it does today. We will present an historical analysis paying close attention to location decisions. Sources include interviews and secondary literature. Second, to map the geographical spread of the cybersecurity industry using Geographic Information Systems. We will map cybersecurity firms in each cluster in the spatial context, to develop the geography and ecosystem scale; and map the firms spread over time. Third, to analyze the role of key stakeholders in developing the industry using network analysis tools. This will include overlaying additional parameters (e.g., size, investments) to create multivariate clustering per firm. Fourth, to analyze the spatial and planning features of the cybersecurity industry. This includes an assessment of the built environment, infrastructure, and physical conditions. Finally, we plan to develop a framework for policymakers.

DETECTING CRYPTOCURRENCY SCAMS AND MEASURING CRYPTOCURRENCY QUALITY

Prof. Neil Gandal and Prof. Marie Vasek

We will research two related issues. The first issue involves developing a methodology and using that methodology to detect cryptocurrency scams. The second issue involves examining the relationship between coin quality and success.

1. Over the past three years, the market capitalization for cryptocurrencies has exploded, soaring from $12 billion in February 2014 to $414 billion in February 2018! Further, the number of coins has increased tenfold in the same period. By 2017, there were more than 1300 cryptocurrencies. Given the rapid changes, it is hard for users to tell the difference between legitimate businesses and frauds. The potential for fraud (cyber-crime) in such an unregulated market is significant. Cyber-crime includes actors deliberately manipulating prices to their own benefit as well as hucksters creating new coins promising benefits that deceive investors. *This is not merely a theoretical risk, as our previous research shows.*
2. Perhaps as the cryptocurrency market develops, scams will be weeded out by people choosing not to invest in them. The second bursting of the bitcoin bubble in 2018 will enable us to address this issue. The (I) rich data, (II) the "ideal natural experiment" of a huge rise followed by a significant fall in the value of the top cryptocurrency and (III) the stark differences between the behavior (returns of the coins) will enable us to examine why the coins behaved differently. With more than 800 coins and repeated observations over time, we will more than enough data to draw meaningful conclusions. If quality, as measured by characteristics indeed explains the returns of the coins, this will show that information in the form of characteristics has an important role to play in terms of weeding out frauds and scams.

We believe that the monetary impact of cyber-crime in the form of Ponzi schemes is large for cryptocurrencies. For instance, Bitconnect, a coin that was once as high as the 7th highest market capacity, in just a day, went from a market capitalization of over $2.5 Billion to collapse. The impact of these scams on consumers is high, particularly for novice consumers who do not recognize the warning signs of a Ponzi scheme. We believe that rooting out these scams at this early stage is important and feasible. By identifying them publicly, we can help stop the mass, largely unknowing, support of them. Cryptocurrency cybercrime matters because – in addition to the victims and the substantial amounts of money may be lost – scams undermine trust in the ecosystem and legitimate cryptocurrencies with innovative business models. We

believe that our work will make an important contribution to a nascent literature on cryptocurrencies and the financial sector.

Future Crimes Enabled by Blockchain-Based Technologies

Dr. Roey Tzezana, Research Fellow Centered Robotic Initiative (HCRI), Brown University, USA

Blockchain technologies are widely accepted to be the 'future of the internet.' These technologies form the basis for Bitcoin's continued existence and success, ensuring that the digital coin system is secure and fraud-free. All the same, some individuals have already discovered ways to manipulate both the bitcoin's value and to hack into related systems to successfully steal digital coins worth hundreds of millions of dollars. Other cyber-criminals took control of Amazon's powerful web services platform and utilized it to mine bitcoins for themselves, and the list of crimes perpetuated on blockchain-based platforms just keeps getting longer every month.

While Bitcoin is the main blockchain-based technology that has gained popularity and public recognition, other blockchain-based platforms are sprouting up by the day. They are usually supported by ICOs – Initial Coin Offerings – which are used to raise hundreds of millions of dollars. In 2017 alone, startups made use of ICOs to raise $5.6 billion. However, almost 10% of the money raised on the most popular blockchain-based platform for start-ups ended up being stolen, using four main methods: exploits, hacks, phishing and Ponzi schemes.

Furthermore, blockchain-based platforms are set to enable a new kind of cloud- organizations, called DAOs – Decentralized Autonomous Organizations. These organizations will in fact be composed of a series of blockchain-based smart contracts that will organize human activities and decision making. One of the best known DAOs, for example, simply called The DAO, was created to allow its members to consolidate their resources and invest together in other start-ups, while making sure the profits are distributed among the investors according to their level of investment. The DAO raised over $150 million in 2016 – only to have 3.6 million ether, corresponding today to more than $3 billion, stolen from it by a cyber-criminal who exploited a vulnerability in the code of The DAO.

Even if DAOs turn out to be resistant to cyber-crime and external hacking, their mere existence enables old crimes to be performed in new and befuddling ways. Consider, for example, the Augur DAO, which is a blockchain-based decentralized prediction market – but which others believe has the potential to become "the greatest gambling platform in history," and which may exist and operate outside of the confines and rule of law of any national government. Augur has already been utilized as an "assassination market," in which people can essentially promise a large payoff for assassinating a certain public figure – with U.S. President Donald Trump being one of the first to have a price on his head.

Other DAOs could be conceived of, which may actually be used to incentivize the public to commit terrorist attacks or hatred crimes, by autonomously delivering money to the perpetrator – with the money coming from thousands of anonymous contributors, and with the government incapable of taking control over the platform or the funds being delivered.

This state of affairs suggests that criminals, hackers and even terrorists are not only contemplating the use of blockchain-based technologies, but are already perverting and hacking currently used platforms. As blockchain-based technologies are only expected to keep on evolving, and the market is expected to grow dramatically, it is critical to conduct research about potential future crimes that could make use of and rely on blockchain-based technologies. Such future crimes need to be considered and analyzed in advance in order to have a prepared response by regulators, law- enforcement bodies, and professionals working in these fields.

In this research, we will develop a better understanding of the security measures and regulations needed to combat the new criminals and crimes, by studying the potential criminal acts that blockchain-based technologies could be used for. We will conduct expert surveys and interviews to create an analytical framework for such crimes, and develop scenarios and policy recommendations.

Twenty-two research grants, awarded in 2016

We published the second Call for Research Proposals in Q1 2016 and received forty-five complete and valid submissions from various disciplines. The two-stage peer review process resulted in awarding funding to twenty-two research projects.

01 Research Grants Awarded in 2016 (ordered by research title)

Title of Research	PI(s)
Adapting QC and MEC algorithms to Anomaly Detection in Big Data	Prof. David Horn
Advanced Attacks Against Internet Security Protocols	Prof. Yuval Shavitt
Avionic Bus Cyber Attack Identification	Avishai Wool; Gabi Shugul; Raz Tikochinski
Best Practices for Verifiably-Correct Concurrent Systems	Noam Rinetzky; Sharon Shoham
Co-Location-Resistant Clouds Security	Prof. Yossi Azar
Compilation Integrity Assurance through Deep Code Alignment	Prof. Lior Wolf
Cyber Jihad Taxonomy: A Qualitative Analysis of the Behavior of Jihadi members on Social Networks and the Jihad Subculture They Create	Udi Sommer; Gahl Silverman
Cyber Threats in Self-Regulating Digital Platforms	Gal Oestreicher-Singer; Ohad Barzilay; Hilah Geva
Detection Of Cyber Attacks In Industrial Control Systems By Intrinsic Sensor Data	Amir Globerson; Matan Gavish; Ronen Talmon
Do firms under-report information on cyber-attacks? Evidence from capital markets	Prof. Eli Amir; Dr. Shai Levi
Identification of Malicious Websites by Learning the Websites' Design Attributes	Prof. Irad Ben-Gal
Multi Robot Coverage and Surveillance	Dan Halperin
Novel Method For Insider Threat Detection	Prof. Ina Weiner
Reconciling Cyber-Security Research with Privacy Law: The Video Analytics and Medical Image Analysis Examples	Prof. Nahum Kiryati
Safety and Privacy of Mobile Applications through Model Inference	Shahar Maoz; Eran Toch; Eran Tromer
Strategic Cyber Reasoning in Attacker-Defender Resource Allocation Games	Ayala Arad; Stefan Penczynski
Symbolic Reasoning for Executable Code	Noam Rinetzky; Mooly Sagiv
The Deniability Mechanism in the Cyber Age – Its Effect on States' Behavior in the International System	Gil Baram
The Interplay of Cyber Vulnerability and Enterprise Credit Risk	Shachar Reichman; Sam Ransbotham; George Westerman

Title of Research	PI(s)
The Intersection Of Cybersecurity And Space Security: New Threats To Cyber-Enabled Space Activities And The Development Of Legal And Policy Responses	Adv. Deborah Housen - Couriel
The Selfish and Caring of Sharing: Exploring the Reasons and Personal Outcomes of Public-Shaming	Prof. Yael Steinhart; Prof. Jacob Goldenberg; Chen Pundak
Towards a theory of cyber power: strategy, public policy, innovation	Lior Tabansky
You can Log-out Any Time You Like, But Can You Ever Leave? Increased Social-Network Usage is Associated with Psychological Distress and Enhanced Cyber Security Risks Among Individuals with Impaired Neural Filtering Ability of Social-Network Information	Gal Sheppes; Roy Luria

Adapting QC and MEC algorithms to Anomaly Detection in Big Data

Principal Investigator: Prof. David Horn, School of Physics and Astronomy, TAU

Project Description:

The Quantum Clustering (QC) algorithm has been developed by us in 2001 and proved to be very successful in various applications. Over the past few years we have demonstrated that its generalization, DQC, can handle well big data and discover unexpected features in them.

Here we propose to further develop QC, and our recently discovered Maximal Entropy Clustering (MEC), to be able to apply both to big data with the particular purpose of anomaly detection. This will hopefully turn out to be a useful tool for anomaly detection in cyber data.

Advanced Attacks against Internet Security Protocols

Principal Investigator: Prof. Yuval Shavitt, Faculty Member, School of Electrical Engineering, Tel Aviv University

Project Description:

We have recently presented DROWN [Usenix'16], a novel cross-protocol attack that can decrypt passively collected TLS sessions from up-to-date clients by using a server supporting SSLv2 as a Bleichenbacher RSA padding oracle.

We suggest in this proposal multiple extensions to this research direction and, in particular, we will try to mount new attacks against modern cryptographic protocols, especially TLS, using our new approach, which is significantly different from classical Bleichenbacher attacks.

Avionic Bus Cyber Attack Identification

Investigators: Avishai Wool; Gabi Shugul; Raz Tikochinski

Project Description:

Avionics bus cyber-attack identification is an embedded cyber solution research project, designed to detect and protect common military avionic buses, in use onboard transport a/c, helicopters, trainers and fighter aircraft around the world. It will address the Blavatnik ICRC 2016 call for research for the topic: "Hardware and embedded systems security, security of IOT". This proposal is for a joint research of Prof. Avishai Wool (TAU faculty of Engineering) and Astronautics C.A. Ltd. (an Israeli company specializing in avionics and military electronics).

Best Practices for Verifiability-Correct Concurrent Systems

Investigators: Noam Rinetzky and Sharon Shoham, Blavatnik School of Computer Science, TAU

Project Description:

Concurrent systems software---such as operating system kernels, hypervisors, database engines, web servers and language run-times---forms the foundation of any modern computer system. It is extremely complex and hard to get right, with bugs making whole services unavailable or opening the doors of seemingly secure systems to viruses and criminals. Ensuring its reliability is thus imperative for building future trustworthy ICT infrastructures.

One of the main difficulties in developing concurrent systems is coordinating between multiple threads competing over shared resources.

Attempts to verify real-world systems software has so far been mostly unsuccessful due to the scale of the systems and the myriad of approaches programmers follow to solve common challenges, e.g., atomic manipulation of a collection data structures.

We suggest to replace the current approach for verifying systems using generic verification tools by techniques which are tuned to formalize and verify the patterns, idioms, abstractions and other forms of structure used to construct concurrent systems.

These patterns are used to ensure various correctness conditions, i.e., to guarantee that certain particularly nasty interactions cannot happen.

Unfortunately, these patterns are described in an informal manner, and hence any proof that following them ensures conformance with a desired correctness condition is implementation-dependent.

We suggest to provide formal, high-level (implementation-independent), definition of best-practices (or policies) that people use in real world software, e.g., certain locking patterns or validation techniques that allow for optimistic manipulation of shared data structures. We will prove that these high-level best practices ensure the intended correctness conditions, and will derive specialized best-practices by means of refinement which would allow to ensure the same to concrete implementations. Further, we plan to design verification and synthesis tools that will support developing software according to the formalized best practices.

The verification tools will prove that a given concurrent module adheres to a desired best-practice and the synthesis tools will take a sequential implementation as an input and generate a concurrent module which respects the intended correctness condition in a provably correct manner.

Co-Location-Resistant Clouds Security

Principal Investigator: Prof. Yossi Azar, Blavatnik School of Computer Science, Tel-Aviv University

Project Description:

We consider the problem of designing multi-tenant public infrastructure clouds resistant to cross-VM attacks without relying on single-tenancy or on assumptions about the cloud's servers. In a cross-VM attack an adversary launches malicious virtual machines (VM) that perform side-channel attacks against co-located VMs in order to recover their contents.

We propose a model for designing and analyzing \emph{secure} VM placement algorithms, which are online vector bin packing algorithms that simultaneously satisfy certain optimization constraints and notions of security. We introduce several notions of security, establishing a connection between them. We also relate the efficiency of the online algorithm to the cost in the cloud computing.

Finally, we propose a secure placement algorithm that achieves our strong notions of security when used with a new cryptographic mechanism we refer to as a shared deployment scheme. This method improves significantly the security of the system.

Compilation Integrity Assurance through Deep Code Alignment

Investigator: Prof. Lior Wolf, Computer Science, TAU

Prof. Lior Wolf is a faculty member at the School of Computer Science at Tel-Aviv University. Previously, he was a post-doctoral associate in Prof. Poggio's lab at MIT. He graduated from the Hebrew University, Jerusalem, where he worked under the supervision of Prof. Shashua. Lior Wolf was awarded the 2008 Sackler Career Development Chair, the Colton Excellence Fellowship for new faculty (2006-2008), the Max Shlumiuk Award for 2004, and the Rothchild Fellowship for 2004. His joint work with Prof. Shashua in ECCV 2000 received the best paper award, and their work in ICCV 2001 received the Marr Prize honorable mention. He was also awarded the best paper award at the post ICCV 2009 workshop on eHeritage, and the pre-CVPR2013 workshop on action recognition. Prof. Wolf research focuses on computer vision and applications of machine learning and includes topics such as face identification, document analysis, digital paleography, and video action recognition.

Project Description:

Hardware is expected to be the root of trust in most products, and embedded threats are the ``new black" in system security. Hardware Trojans, on which we focus, are both persistent and extremely hard to detect. In this project, we address the problem of executable component addition, substitution, and re-programming in the supply chain.

We propose a completely novel approach for detecting hardware Trojans. We obtain, from the foundry or by other means the binaries. These binaries are expected to largely match the programming code provided by the hardware designer with some unavoidable additions inserted in order to support debugging, QA, and to comply with manufacturing constraints. We then identify for every line of the binaries (viewed as assembly code) the matching line in the original C code. Following this step, we can easily identify insertions and other forms of modifications. The engineers of the supplier company or any other verifying agency can then readily track these modifications and tag each one as malicious or not.

Cyber Jihad Taxonomy: A Qualitative Analysis of the Behavior of Jihadi members on Social Networks and the Jihad Subculture They Create

Principal Investigators: Udi Sommer and Gahl Silverman, TAU

Project Description:

In an era of a global war against Islamic extremist terrorism, a major element has become the increasing presence of terrorist groups online. 'Cyber Jihad' that has proliferated, simultaneously with the significant growth of social networking sites, has become an enormous challenge and ushered in a new and terrifying era (that includes most recently the attacks in Paris, Brussels, Orlando and Nice).

Previous studies in this field, applied quantitative approaches to developing an algorithm or to draw a global map of connections between distinct terrorist organizations. However, existing work largely disregarded the aspect of individual extremist Muslims, their behavior, activity patterns and thus the jihad subculture they form online, which provides the infrastructure for terrorist activity.

The proposed study will use a holistic qualitative approach, assisted by a mixed methods analysis software (NVivo11), to apply a two-stage inquiry in order to: (1) identify the characteristics of a potential Jihadi terrorist; (2) identify the taxonomy of the discourse between Jihadi members; and (3) create a categorization of posts and replies that exhibit or inspire an implied preliminary jihadi terrorists' behavior (see figure 1). The analytic leverage will then allow us to zoom in on the individual level and to draw a multilayered picture of cyber jihad subculture and the basis it sets for broader online terrorist activity.

Cyber Threats is Self-Regulating Digital Platforms

Investigators: Gal Oestreicher-Singer; Ohad Barzilay; Hilah Geva, Coller School of Management, Tel Aviv University

Project Description:

In the classic movie WarGames (1983), a computer is granted control over the US ballistic missile system. Towards the end of the movie, the computer attempts to launch those missiles after drawing false conclusions about hostile actions of the Soviet Union. The movie raised an important issue, which we wish to investigate further in contemporary settings: the benefits and hazards resulting from allowing computer algorithms to regulate and govern digital platforms. In the proposed research we use state-of-the-art methods and develop novel approaches of our own to study the economic consequences of allowing a digital market to automatically approve sellers who submit products to that market. We aim to provide policy makers and platform stakeholders with new insights regarding the expected revenues and quality shifts that result from a digital platform's self-regulation.

Detection of Cyber Attacks in Industrial Control Systems by Intrinsic Sensor Data

Investigators: Amir Globerson; Matan Gavish; Ronen Talmon

Project Description:

Recent years have seen an explosive increase in cyber-attacks against industrial control systems (ICS), including power stations, power grids, dams and water utilities. Cyber-attacks on such systems can have disastrous effects, and any industrialized nation must build an infrastructure for detecting such attacks and deflecting them. In the proposed research we assume the worst-case-scenario in which an attack has already gained control, and even hijacked the sensors of a monitored ICS. We propose to develop a last line of cyber defense: an ICS Takeover Detection System (ICS-TDS), aimed to detect a cyber-takeover of the monitored ICS, even in the presence of successful sensor hijacking.

Our approach will rely on detailed non-linear models of the dynamics of the ICS, based on manifold methods, deep learning, graphical models and high dimensional statistics.

The PIs bring complementary expertise to the problem, which is expected to yield both effective cyber defense tools, as well as new machine learning methods for dynamical systems.

The Deniability Mechanism in the Cyber Age – Its Effect on States' Behavior in the International System

Principal Investigator: Gil Baram, Department of Political Science, Tel-Aviv University

Project Description:

Although the nature of the cyber threat is open for discussion, one cannot ignore its effect on the characteristic of war and the relations between states. Most research so far has only dealt with one side of the equation, namely – how states attribute attacks to other nations and how they verify and prove their accusations. However, almost no research has been done on the opposite side of the equation, i.e., how states successfully manage to deny their responsibility for alleged cyber-attacks and evade accusations that they were responsible for committing an attack. This research will deal precisely with this topic. By using several quantitative and qualitative techniques, this research seeks to examine how does the use of the deniability mechanism affects the degree of aggression of states in the international arena. The ultimate purpose of this research is to create a theoretical framework that will allow for a better understanding of how the use of offensive cyber warfare technology affects the relations between states and the lack of visible long-term conventional war.

Do Firms Under-Report Information on Cyber Attacks? Evidence from Capital Markets

Investigators: Prof. Eli Amir; Dr. Shai Levi

Project Description:

Firms should disclose information on material cyber-attacks. However, because managers have incentives to withhold negative information, and investors cannot independently discover most cyber-attacks, firms may underreport cyber-attacks. Using data on cyber-attacks that were voluntary disclosed by firms and those that were withheld and later discovered by sources outside the firm, we estimate the extent to which firms withhold information on cyber-attacks. We find that withheld cyber-attacks are associated with a decline of approximately 2.6% in equity values in the month they are discovered, and disclosed attacks with a substantially lower decline of 0.6%. The evidence suggests that managers do not disclose negative information below a certain threshold, and withhold information on the more severe attacks. Using the market reactions to withheld and disclosed attacks, we estimate that managers disclose information on cyber-attacks when investors already suspect that in high likelihood (46%) an attack has occurred. Our results suggest there is underreporting of cyber-attacks, and imply that if regulators wish to ensure that information on attacks reaches investors, they should consider tightening mandatory disclosure requirements.

Identification of Malicious Websites by Learning the Websites' Design Attributes

Principal Investigator: Prof. Irad Ben Gal, Department of Industrial Engineering, TAU

Project Description:

Malicious software (malware) is a challenging cyber security threat, as it is commonly bundled within software that is actively downloaded by naive users. A major source for malware downloads are Crack websites that are used to circumvent copyright protection mechanism. Crack websites often change URLs and IPs to avoid automatic detection, but in many cases they preserve specific visual designs that signal on the websites function to potential users. Exact categorization of these design features is challenging due to the huge volume of information on the used shapes, colors, text fonts, sizes etc. In this research we suggest a machine learning procedure for automatically identifying crack websites. Based on a primary model, we show that classification by HTML colors and design features can reach an accuracy of over 90% in some cases. Adding metadata, such as webpage keywords, enhances the accuracy in the tested dataset. We show how conventional machine learning models can be used to classify suspicious websites by learning their design features that are often overlooked and obtain results in the context of developing intelligent cyber security mechanisms. The main purpose of this work is to strengthen the preliminary results and scale the developed algorithms to analyze large number (millions) of websites automatically.

The Interplay of Cyber Vulnerability and Enterprise Credit Risk

Investigators: Dr. Shachar Reichman; Sam Ransbotham; George Westerman

Project Description:

Cyber-attacks occur on a daily basis worldwide, directly affecting the stability of organizations everywhere. With increasingly internally and externally interconnected operations and computer systems, there are both direct and indirect effects of security compromises. The effects of cyber-attacks cascade through the entire ecosystem, resulting not only in direct costs of repairing and restoring the systems, but also in delays and halts of services and operations and, potentially, a loss of reputation and decrease in future business activity.

Considering the extensive literature on the economics of information security, it is somewhat surprising that when estimating a firm's credit rating, a core measure of financial stability, credit rating agencies espouse the importance of information security, yet ironically still do not include security in the firm credit rating

This research aims to develop a novel method to evaluate the interaction between cyber vulnerability and enterprise financial risk as reflected by its credit rating. Using multiple data from online financial and security sources we will explore the effect of a firm's cyber factors, including DNS hacking events, intrusion risks, exposure to DOS attacks, servers' configuration levels, and privacy measures, on its credit rating. We will then examine the counter effect, how a credit rating downgrade affects the firms' information security measures.

The Intersection of Cybersecurity and Space Security: New Threats to Cyber-Enabled Space Activities and the Development of Legal and Policy Responses

Principal Investigator: Adv. Deborah Housen-Couriel, LL.M, MPA,

Project Description:

One of the most compelling interdisciplinary challenges to cybersecurity at present is also a hitherto under-researched one; that is, the intersecting threat vectors in cyberspace and in outer space with which states and private entities are currently engaging. These vectors converge around the present vulnerabilities of satellites and the data transmitted by satellite communications, which take place almost entirely through cyberspace. The proposal detailed below addresses the intersection of cybersecurity and space security at the three levels of legal analysis, governance regimes and present and future public policy.

Novel Method for Insider Threat Detection

Principal Investigator: Prof. Ina Weiner, Professor of Psychology TAU

Project Description:

This exploratory track proposal addresses the issue of insider threat, proposing a novel approach to detection of malicious insiders' illicit activities. While cyber-attacks are typically connected with outsiders' attacks, it is becoming increasingly recognized that an equally great threat to an organization's security lies within. Existing surveillance methods, including behavioral analytics, cannot effectively defend against malicious insiders because they have authorized access to data. I propose to develop a novel approach for detecting malicious insiders' activity, namely, an unobtrusive monitoring, by means of a standard webcam, of changes in pupil size, an involuntary response that is produced when people are aroused, stressed and/or recruit their attentional and cognitive resources as is the case when they are performing illicit acts. The unique advantage of the pupillary response is that it is universal, and cannot be controlled voluntarily. Therefore, an unobtrusive measurement of pupil size is a perfect candidate for detecting a change in emotional arousal and cognitive effort that cannot be suppressed deliberately, and using this signal for alerting the system of a potential threat. To date, there is no method for monitoring pupil size using a standard web camera in real time. The development of such a method is the aim of this exploratory proposal.

Multi Robot Coverage and Surveillance

Investigator: Prof. Dan Halperin, Blavatnik School for Computer Science, TAU

Project Description:

We propose to devise and analyze novel efficient algorithms for multi-robot motion coordination, where a fleet of robots is carrying out tasks of coverage and surveillance.

Monitoring and surveillance by fleets of robots is a burgeoning trend around the globe targeting a wide range of tasks from wildlife protection through mine detection to border patrolling. In recent years our group has been in the forefront of developing efficient methods for robot motion planning, for optimizing motion plans, and for dealing with generalized variants of multi-robot motion. We plan to harness techniques from algorithmic robotics and computational geometry and to develop new tools for a family of multi-robot tasks related to tracking and monitoring, tools that will be at once practically efficient and backed by theoretical analysis.

Reconciling Cyber-Security Research with Privacy Law: The Video Analytics and Medical Image Analysis Examples

Principal Investigator: Prof. Nahum Kiryati, Professor at the School of Electrical Engineering, TAU

Project Description:

Research and development (R&D) in video content analysis, medical image analysis, and other data analysis techniques related to anomaly detection, require huge amounts of data for training and evaluation. This is underscored by the groundbreaking deep-learning paradigm. The only practical source for relevant data is collections of real data acquired in the field. In the context of video content analysis, this refers to actual video surveillance databases acquired in public areas. Such data is strictly protected by privacy regulations. Consequently, its use for R&D is practically limited to large corporate entities that handle the data as part of their business. These include surveillance system providers, cloud services and social networks. Academic research on these topics is therefore crippled, and new industrial players are also excluded. In the context of medical image analysis, the relevant data is the collection of medical images stored in Picture Archiving and Communication Systems (PACS) at hospitals. Access to this resource is usually available to hospital staff only, creating an effective data monopoly with respect to external academic and industrial players. The proposed research, at the interface between technology, law and policy, will evaluate the problem and develop interdisciplinary solutions, facilitating academic R&D in video content analysis, medical image analysis and similar cyber-security anomaly-oriented data analysis challenges.

Symbolic Reasoning for Executable Code

Investigators: Prof. Mooly Sagiv and Dr. Noam Rinetzky, Blavatnik School for Computer Science, TAU

Project Description:

Modern society fundamentally relies on software systems, with some of its most vital processes, such as communication and banking implemented in software.

Hence, the security of these systems is paramount, as otherwise a malicious party can take down critical national infrastructures or lead them to incorrect, possibly disastrous, behaviors. A key reason for the vulnerability of software systems is that ensuring that they behave correctly for any given input is provably impossible. This opens the door for sophisticated users to design unexpected, yet seemingly benign inputs that can derail an attacked system into an undesired execution path.

Our goal is to develop tools, techniques, and methodologies that help detect vulnerabilities in realistic software systems by synthesizing inputs that can force a program to go from one given program point to another, or determine that no such input exists, and hence that this particular vulnerability never occurs. We plan to do so by expressing the feasibility of an execution path using a logical formula and harnessing the power of modern symbolic SAT solvers, e.g., Z3, to identify a satisfying assignment, i.e., an input scenario which exposes the vulnerability, or determine that none exists. Indeed, tools such as SAGE, KLEE, and uc-KLEE show that such symbolic reasoning can be very useful in generating tricky inputs. However, scaling these tools to realistic software is difficult: Firstly, determining the existence of an execution path is an undecidable problem and even checking whether a given path formula is feasible is NP- complete. Secondly, the limits of the logical theories underlying the solver make it challenging to handle many aspects of low level code including non-linear arithmetic, pointers, loops, and indirect jumps. Finally, the code can be simply too big for current techniques.

In this project, we will scale the ability of tools, such as KLEE, to more realistic situations by pursuing several intertwined directions:

1. Simplifying the generated logical formulae using sound information obtained from static program analysis
2. Designing domain-specific theories suitable for reasoning about low-level code
3. Making the reasoning modular by developing symbolic procedure summaries
4. Leveraging high-level guidance from the user to identify promising code parts to explore.

Safety and Privacy of Mobile Applications through Model Inference

Investigators: Shahar Maoz; Eran Toch; Eran Tromer

Project Description:

Mobile operating systems pose serious security and privacy threats and therefore can compromise the smart city and degrade trust between citizens and governments. In this proposal, we develop AppMod, a model-based framework for safe mobile applications on the Android platform. The approach relies on dynamic analysis of apps, uses model-based inference and differencing to detect privacy violations and behavioral anomalies, and suggests new interactions that allow users to effectively control their privacy and security.

This project represents a 3-year collaboration between five researchers at Singapore Management University (SMU) and Tel Aviv University (TAU): Lo (SMU), Maoz (TAU), Gao (SMU), Tromer (TAU), and Toch (TAU). Lo and Maoz are experts in model inference and differencing, while Gao, Tromer, and Toch are experts in cybersecurity. Gao and Tromer have much experience in building secure infrastructures, while Gao and Toch have in-depth knowledge on realizing effective user interaction models for making security accessible to everyone.

The Selfish and Caring of Sharing: Exploring the Reasons and Personal Outcomes of Public-Shaming

Principal Investigators: Prof. Yael Steinhart, Prof. Jacob Goldenberg and Dr. Chen Pundak TAU

Project Description:

Public-shaming has long been a dubious tool for justice, punishment and education. In recent years, social networks have increased its spreading, availability and popularity. Shaming usually includes broadcasting of personally identifiable information about an individual been shamed. While public-shaming can be used to violate the right to privacy and dignity, it can also be seen as informal way to force social control to prevent deviant behavior. The existence of these two possible outcomes (i.e., the possibility of improving something

by hurting someone) emphasizes the complexity of public-shaming and the need to further understand its drivers and consequences.

The proposed research will focus on public-shaming that runs through social networks. It will include a series of studies to explore the motivations and outcomes of public-shaming. We hypothesize that: (1) vulnerability to one's self-image will increase the likelihood of joining active shaming, especially when the wrongdoer is perceived to be similar to the 'shamer'; (2) self-image perceptions will increase after taking part in online shaming; (3) shaming will occur when its goal leans toward expressing the 'shamer's identity rather than toward fulfilling functional needs; (4) morality will drive public-shaming when the wrongdoer is non-identified rather than identified.

We have already conducted two pilot online experiments showing that the likelihood of joining public-shaming enhances one's self-esteem. In future studies, in lab settings and in the field, we will include measures related to social norms, morality, self-expressiveness and superiority as possible mechanisms that may explain the willingness to take part in public-shaming.

Strategic Cyber Reasoning in Attacker-Defender Resource Allocation Games

Investigators: Ayala Arad, Coller School of Management at TAU; Prof. Stefan Penczynski, University of Mannheim

Project Description:

Resource allocation games provide a natural environment in which to explore the strategic aspects of cyber security. Computer systems at risk in the financial, industrial, military, and private sectors are becoming increasingly complex, consisting of multiple components and exhibiting a variety of attack surfaces or vulnerabilities, such as backdoors, denial-of-service attacks, Trojans, phishing, direct-access attacks, etc. In either attacking or defending on these "battlefields", resources might be given and limited or determined by the players' choices.

In the proposed research, we develop extensions of the popular Colonel Blotto game with application in cyber security and study cyber-attacker and defender strategic reasoning experimentally. The project is expected to provide defenders with some basic principles for allocating security costs across various components of a system when defending against anonymous attackers. Furthermore, based on the experimental results, we intend to construct an equilibrium-like solution concept, which takes into account that players use categorical thinking or multi-dimensional reasoning. The solution concept is expected to be particularly useful for predicting behavior in situations of repeated interaction between a particular defender and attacker, where both players become more sophisticated over time and learn from their opponent's previous actions, although they are subject to certain cognitive or computational limitations.

Towards an Interdisciplinary Unified Theory of Cyber Power: Security Studies, Meta-Governance, National Innovation System

Principal Investigators: Prof. Isaac Ben-Israel and Lior Tabansky, Blavatnik ICRC.

Project Description:

Cyber security science is different: it is a science in the presence of adversaries. Exact sciences help understand the technology. Social science scholarship may help to better understand the actors – but it is underutilized. We identify and develop state-of-the-art scholarship in three topical thrusts, and then integrate these theoretical building blocks to develop an interdisciplinary unified theory of Cyber Power which is generalizable to multiple settings.

Security Studies: The Revolution in Military Affairs analytical framework.

Public Policy: Meta-Governance and non-traditional policy instruments.

Political Economy: National Innovation Systems (NIS)

This proposal builds on the exploratory research grant awarded to Lior Tabansky in 2015, which has resulted in a book and a peer-reviewed article.

The science of cybersecurity will benefit from an interdisciplinary unified theory of Cyber Power, a theory addressing the actors as well as the technology.

You can Log-out Any Time You Like, But Can You Ever Leave? Increased Social-Network Usage is Associated with Psychological Distress and Enhanced Cyber Security Risks among Individuals with Impaired Neural Filtering Ability of Social-Network Information

Principal Investigators: Prof. Gal Sheppes and Prof. Roy Luria, School of Psychology, TAU

Project Description:

Half a billion Facebook (FB) users log-in multiple times a day and spend 18 minutes on average each visit. Although this statistic raises significant worries that increased usage may be associated with maladaptive psychological consequences such as anxious and depressive symptoms, existing studies provide mixed results. We suggest that individuals vary in their ability to control FB cues when such cues interfere with performing goal directed activities. For example, some individuals may fail to overcome the urge to click an open FB tab when working on a school project. We argue that for these individuals in particular, enhanced FB usage may be associated with maladaptive psychological elements. Accordingly, the main premise of this research program is that enhanced FB usage would lead to increased anxious and depressive symptoms, mainly among individuals with impaired ability to filter potent FB information when this information is incongruent with one's goals. We further argue that an increased anxious and depressive state would be associated with greater self-disclosure web behavior, which exposes users to heightened cyber security threats. The present research proposal advances prior studies in developing a novel paradigm that directly isolates the online neural mechanism of filtering irrelevant FB information, and in measuring actual FB usage and psychological measures in the laboratory and in daily life across time. Accordingly, the present research program has two main goals that will be tested in two large studies (total n=240). Study 1 will examine the first main goal, predicting that the relationship between laboratory short-term enhanced FB usage and immediate anxious and depressive symptoms, will be mostly evident in individuals with impaired neural FB filtering ability. Study 2 will further show that among individuals with impaired neural FB filtering ability, enhanced FB usage in daily-life would lead to increased long-term anxious and depressive symptoms and self-disclosure web behavior that increases cyber risks ranging from cyber bullying to identity theft. Preliminary findings support the aforementioned conceptual logic of the proposal. Expected benefits include shedding light on when and why certain individuals that excessively use social-networks, experience immediate and long-term maladaptive psychological consequences that also expose them to significant cyber security threats.

Thirty-four research grants, awarded in 2014

The first Call for Research Proposals has achieved the just-established Blavatnik Interdisciplinary Cyber Research Center's first goal: finding and supporting researchers throughout the University, explicitly including those in Social Sciences, Law and Business schools. The two-stage peer review process resulted in awarding thirty-four research grants, establishing Tel Aviv University as the largest and most diverse research institution in Israel.

03 Research Grants Awarded in 2014 (ordered by research title)

Research Title	Principal Investigator(s)
Confess or Deny? Strategies for Dealing with Cyber Attacks	Dr. Deganit Paikowsky
Violence and the (Social) Construction of Cyber Deterrence	Dr. Amir Lupovici
Cyber, Space and Nuclear Weapons Analogies, Interrelations and Differences in forming National Strategy – A Comparative Analysis of the United States and Russia (USSR)	Dr. Amir Lupovici + Dr. Dimitry (Dima) Adamsky
Cybersecurity Theory Development: the Israeli Case in Strategic Context	Mr. Lior Tabansky, M.A.
Hostile Influence Operations via Social Media: A Cybersecurity Issue? Assessing the Applicability of Recent Evidence to the Israeli Soft Power	Mr. Lior Tabansky, M.A.
What's the Value of Bug Bounty Programs? Bug Bounty	Ms. Keren Elazari
Economic Utilization of Workforce-Based Labeling for Security Applications	Dr. Tomer Geva
Mitigating the Risk of Advanced Cyber-Attackers	Dr. Ohad Barzilay + Prof. Asher Tishler
The Effect of Engagement on Private Information	Prof. Gal Oestreicher-Singer
Non-Public Financial Information Leak	Dr. Roy Zuckerman
Cyber Information Sharing in a Competitive and Conflicted Environment	Mr. Aviram Zrahia, MBA
Cyber Security Technology Foresight	Dr. Tal Soffer
Crime and IoT	Dr. Roey Tzezana
Alternative Enforcement in Cyber Space	Dr. Haim Wismonsky
Balancing National Security and Privacy Rights to Privacy and the Rule of Law in Democratic Societies a Comparative Analysis	Adv. Deborah Housen-Couriel
Attack Resilient Resource Placement in Cloud Computing System and Power Grid	Dr. Hanoch Levy
Anonymous and Secure Electronic Voting Protecting our Democratic Infrastructure	Dr. Amnon Ta-Shma + Prof. Alon Rosen
Securing Servers and Endpoints using Software Guard Extensions	Prof. Sivan A. Toledo + Dr. Eran Tromer
Extracting Signatures and Filters for Zero-day Sophisticated DNS and other DDoS Attacks	Prof. Yehuda Afek + Prof. Anat Bremler-Barr

Research Title	Principal Investigator(s)
Infrastructure for Cyber Threat Information Sharing	Prof. Tova Milo + Dr. Daniel Deutch
Anomaly Detection for Critical Infrastructure Protection: Second Generation Duration 4 Years	Prof. Amir Averbuch
Robust Decentralized Digital Currency	Dr. Iftach Haitner + Dr. Amos Fiat + Dr. Eran Tromer + Dr. Benny Applebaum
Guiding and Incentivizing Cyber-Security Behavior	Dr. Eran Toch
Network Attack and Detection in Modbus/TCP SCADA Systems	Prof. Avishai Wool + Dr. Leonid Lev
Photonic Emission Side-Channel Cryptanalysis of Secure Hardware Devices	Prof. Avishai Wool
Understanding IP Hijack Events	Prof. Yuval Shavitt
Ultra long Fiber Laser for Secure Communications	Prof. Jacob Scheuer
Personal Genomic Data: Privacy and Security Aspects	Prof. Benny Chor + Dr. Metsada Pasmanik-Chor
Evolving Cyber-Threats and Countermeasures: Mathematical, Behavioral and Legal Perspectives	Prof. Joachim Meyer + Prof. Ronen Avraham
Privacy by Design by Legislation	Prof. Michael Birnhack + Dr. Avner Levin
Shocks to and Security in the Bitcoin Ecosystem: An Interdisciplinary Approach	Prof. Neil Gandal + Dr. Tyler Moore
A Machine Learning Collaborative Study of Language-Action Cues for Spontaneous Deceptive Communication and Cyber-Ontology Development	Prof. Oded Maimon + Prof. Shuyuan Mary Ho
Smart Cities Cyber Security (SCCS)	Prof. Michael Birnhack + Prof. Issachar Rosen-Zvi + Dr. Tali Hatuka

* Amount received for two or three-year project.

Alternative Enforcement in Cyber Space

Principal Investigator: Dr. Haim Wismonski

Project Description:

The proposed research question is: How to properly run an alternative legal measure in order to defend against damage caused by criminal offenses in cyberspace, alongside the measures taken today as part of the "classical" criminal investigation in cyberspace.

Anomaly Detection for Critical Infrastructure Protection: Second Generation

Principal Investigator: Prof. Amir Averbuch

Project Description:

The primary goal of this proposal is to develop methodologies (theories, algorithms, software and systems) to detect anomalies in an unstructured HDBD, which can be the underlying signs of malware, zero day attacks or operational malfunctions, or both, that can impact critical infrastructure.

Anonymous and Secure Electronic Voting Protecting our Democratic Infrastructure

Principal Investigators:

Prof. Amnon Ta Shma; Prof. Alon Rosen

Project Description:

The investigators believe the transition to electronic voting is inevitable and that there is no alternative to software-independent voting. They are studying the delicate security issues involving electronic voting and the money needed for implementing and testing such a system.

Attack Resilient Resource Placement in Cloud Computing System and Power Grid

Principal Investigator: Dr.. Hanoch Levy

Project Description:

This research will extend the methodology and devise algorithmic solutions which will provide resource placement strategies that will be efficient and optimal with respect to malicious environments. In the context of cloud computing, the investigators will capture the volatility of the resources due to attacks by modeling the resources, namely the L_i variables, as random variables, whose value depends on the number of resources the designer placed in the i-th site as well as on the probability that they fail (due to attacks). Since in previous work, the L_i variables were deterministic, this will require a significant generalization of the model and the analysis approach using tools from stochastic analysis, optimization and graph algorithms. It is expected that the analysis will reveal the number of resources, the types of resources and their locations, such that resilient service is provided, while taking into account the cost and performance of services in regular operation. This analysis will provide insight into the tradeoffs between resilience to attacks and level of service in regular operation and cost.

Balancing National Security and Privacy Rights to Privacy and the Rule of Law in Democratic Societies, a Comparative Analysis

Principal Investigator: Adv. Deborah Housen-Couriel

Project Description:

The research focuses on the means of defense against and the effects of the cooperation between shields and the attack on the decision-making system.

Confess or Deny? Strategies for Dealing with Cyber Attacks

Principal Investigator: Dr. Deganit Paikowsky

Project Description:

In recent years, there have been many cyberattacks on critical systems and national infrastructures. These attacks have become more complex and have a great impact on governments, economy and industry. Generally, it is assumed that the cyber world is easier to attack than defend. However, current research in security and social sciences rarely engage in strategies for protection against cyber-attacks.

Crime and IoT

Principal Investigator: Dr. Roey Tzezana

Project Description:

The investigators suggest developing a better understanding of the security measures and regulations needed to combat new criminals and crimes, by studying the possibilities the IoT holds for criminal acts, conducting expert surveys to estimate timelines for the feasibility of certain crimes, developing high damage-potential scenarios for future crimes and providing the regulators and the Israeli police with policy advice on how to prepare for said crimes.

Cyber Information Sharing in a Competitive and Conflicted Environment

Principal Investigator: Mr. Aviram Zrahia

Project Description:

The problem this research addresses is how to reduce the level of objection and increase the level of cyber information sharing between parties in a competitive and conflicted environment. The goal of this research is to develop a model for sharing cyber information in a competitive environment, which could be integrated into existing and evolving sharing methodologies. The importance of this research is in finding a way for competing parties, whether commercial organizations or nations, to enhance their overall cyber-security capability to fight the cyber war by cooperating despite their conflicting interests.

Cyber, Space and Nuclear Weapons Analogies, Interrelations and Differences in Forming National Strategy – A Comparative Analysis of the United States and Russia (USSR)

Principal Investigator: Dr. Amir Lupovici, Dr. Dimitry (Dima) Adamsky

Project Description:

This study is aimed at portraying and analyzing major synergies, analogous and anomalies of American and Russian national strategy concerning the three most advanced technological strategic fields: cyber, space and nuclear weapons. It is achieving this by means of mapping the various actors, processes, mechanisms and strategies that influence the forming of American and Russian policy in each of these fields, comparing them and then analyzing the similarities, major differences, and interrelations.

Cybersecurity Technology Foresight

Principal Investigator: Dr. Tal Soffer

Project Description:

The main goal of this study is to derive the current cyber security technology status from the analysis of popular standards such as NERC-CIP. Based on this analysis, a foresight process is being carried out in order to assess future directions and emerging technologies in cyber security, within the time-frame of the next 10-15 years. Attention is being paid also to new cyber-threats that may emerge within this period. The process includes an expert survey that can be repeated and reported on a yearly basis.

Cybersecurity Theory Development: the Israeli Case in Strategic Context

Principal Investigator: Mr. Lior Tabansky

Project Description:

The Israeli cyber-defense capability is held in high regard. Could we generalize a roadmap to achieve a consistently excellent state of national cybersecurity from this case? Public discussions on Israeli cybersecurity are, however, usually detached from strategic context, impeding cybersecurity scholarship and policy efforts. We argue that the common explanations of cybersecurity as a by-product of military technology, entrepreneurial skills or innovative ICT sector are only manifestations of other variables. Uncovering the links between the Israeli grand-strategy and its cybersecurity policy will improve analytical tools and have policy implications.

Economic Utilization of Workforce-Based Labeling for Security Applications

Principal Investigator: Dr. Tomer Geva

Project Description:

This research examines the strategic importance and the impact of network structure and the effect of uncertainty and risk aversion on the validity of the negotiating process.

The Effect of Engagement on Private Information

Principal Investigator: Prof. Gal Oestreicher-Singer

Project Description:

In this research proposal, it is hypothesized that engaged users will agree to reveal more personal information as compared to the less engaged and that compliance with a website's requests for engagement will lead to subsequent information revelation. This exploratory research can improve our understanding of the process of information revelation as well as increase user awareness to pitfalls and help policy-makers in the field of privacy to make more informed decisions regarding website design for privacy.

Extracting Signatures and Filters for Zero-day Sophisticated DNS and other DDoS Attacks

Principal Investigators: Prof. Yehuda Afek; Prof. Anat Bremler-Barr

Project Description:

Over the past three years, the first two PIs with their students have developed algorithms for zero-day signature extraction for html based DDoS attacks and the goal of this proposal is to extend this work in several directions. This proposal entails the development of new algorithms for the analysis of high throughput streaming data (Big Data) to detect heavy hitters with high distinct counts that were not such at peace time, i.e., are very likely malicious and not legitimate.

Evolving Cyber-threats and Countermeasures: Mathematical, Behavioral and Legal Perspectives

Principal Investigators: Prof. Joachim Meyer; Prof. Ronen Avraham

Project Description:

This research addresses a set of interrelated research questions, combining analytical (optimization), behavioral (experimental economic and psychology) and legal perspectives. From a behavioral modeling perspective the investigators are developing quantitative models to predict users' behavior in environments with changing threats and information about threats and they are validating the models with empirical studies. Under what conditions will end-users be particularly vulnerable to attacks? What will affect the end-user's motivation to prevent security threats? The research will then be extended, addressing questions such as, what advice, alerts or nudges can be used so that end-users respond positively to this information, avoiding "cry wolf" and information-overload effects, due to which users cease to respond to indications (Akhawe & Porter Felt, 2013)? These questions will then be addressed from a legal perspective, asking about rules for warning end-users in a rapidly changing environment: when should, for instance, companies be required to alert end-users about emerging threats, to delete end-user accounts because using them may create a risk for the end-user, to cease marketing a service because it can be used to attack end-users, etc.? In this context, the investigators will consider the results from the analytic and behavioral parts, trying to predict how different policies regarding the issuing of alerts will affect the overall outcomes at the individual user and at the system level.

Guiding and Incentivizing Cyber-Security Behavior

Principal Investigators: Dr. Eran Toch

Project Description:

In this project, the investigator is conducting theoretical and empirical research with two objectives in mind: first, to propose and evaluate a theory that explains users' decision-making given negative and positive incentives and second, to test how we can influence users' decision-making processes by designing gamification-based incentive systems. By the end of the study, the investigator plans to offer a toolkit for the optimal design of incentive systems for cyber-security that enhances user involvement in the interaction in enterprise security systems.

Hostile Influence Operations via Social Media: A Cybersecurity Issue? Assessing the Applicability of Recent Evidence to the Israeli Soft Power

Principal Investigator: Mr. Lior Tabansky

Project Description:

This interdisciplinary research aims to develop a new analytical framework for cyber power and cybersecurity, explicitly including defense against hostile influence operations. It builds on the work done during the 2013 internship of Margarita Jaitner from the Swedish Defence College with Mr. Tabansky at the Yuval Ne'eman workshop.

Infrastructure for Cyber Threat Information Sharing

Principal Investigators: Prof. Tova Milo; Dr. Daniel Deutsch

Project Description:

The goal of this project is to develop solid scientific foundations for large-scale cyber threat information sharing and analysis. The investigators believe that such a principled approach is essential in order to obtain knowledge of superior quality, to realize the task more effectively and automatically to be able to reuse solutions and thereby to improve the effectiveness of defensive cyber operations and incident response activities.

A Machine Learning Collaborative Study of Language-Action Cues for Spontaneous Deceptive Communication, and Cyber-Ontology Development

Principal Investigators: Prof. Oded Maimon; Prof. Shuyuan Mary Ho

Project Description:

In this study, the use of deceptive language is being examined and language usage patterns during online deceptive acts explored. As interpersonal communication is defined as a dynamic exchange of messages between or among two or more people, the research focuses on social interactions where participants try to mutually influence each other in a dynamic fashion. The investigators are thus seeking an answer to the following research question: what linguistic cues can be attributed to deception in a computer mediated communication across a pluralistic background of users?

Mitigating the Risk of Advanced Cyber-Attackers

Principal Investigators: Prof. Asher Tishler, Dr.. Ohad Barzilay

Project Description:

The proposed research examines some aspects of the new rules. The investigators aim to draft formal analytical opportunities for the attacker and the respective challenges faced by the defender. They intend to use the tools of game theory, decision problems and optimization as well as economic tools to analyze the attack scenarios and various protection and optimal coping strategies formulated according to certain parameters.

Non-Public Financial Information Leak

Principal Investigator: Dr. Roy Zuckerman

Project Description:

This research proposes an exploratory study of the role of cyber security in non-public information leaks. This study examines whether firms properly oversee the online security measures taken to protect non-public financial information both within the organization and with the affiliated service providers. In addition, the investigators are attempting to identify certain service providers which are more likely to be associated with leaks and determine if they are associated with weak cyber security measures. This is the first study to highlight the risk of trading based on non-public information obtained via cyber hacks. As such, policy implications based on the findings of such a study may be far-reaching.

Network Attack and Detection in Modbus/TCP SCADA Systems

Principal Investigators: Prof. Avishai Wool; Dr. Leonid Lev

Project Description:

This research is comprised of several tasks:

1. Developing network penetration-test tools specifically for the Modbus SCADA protocol.
2. Experimentation with the penetration tools.
3. Testing the model-based anomaly-detection system on data from the IEC HEDVa environment and from U.Twente.
4. Testing the anomaly-detection system against the penetration tools.

Photonic Emission Side-Channel Cryptanalysis of Secure Hardware Devices

Principal Investigator: Prof. Avishai Wool

Project Description:

The goal of this work is to apply the methods and know-how developed on the power-analysis side-channel and apply them to the photonic emission side channel. The TAU and Berlin teams already have a good working relationship and would like to collaborate on this topic. It is believed that a solver-based approach allows for a much better description of the very detailed information leakage which can be exposed by the photonic side channel.

Personal Genomic Data: Privacy and Security Aspects

Principal Investigators: Prof. Benny Chor; Dr. Metsada Pasmanik-Chor

Project Description:

The current research employs the tools of game theory, decision and optimization problems and economic tools to analyze scenarios.

Privacy by Design by Legislation

Principal Investigators: Prof. Michael Birnhack; Prof. Avner Levin

Project Description:

Privacy is a key element in cyber security. Protecting personal data held and processed by cybernetic systems converges with other security principles and may enhance data subjects' and end-users' trust in such systems, resulting in greater acceptance thereof. Violations of privacy, on the other hand, will diminish trust, acceptance and efficiency of cyber systems. However, privacy and security are not fully congruent concepts and at times, privacy requires taking measures that might limit the functionality and usability of technological systems. This research asks "How can a cybernetic system achieve the optimal combination of usability, security and privacy"?

Robust Decentralized Digital Currency

Principal Investigators: Dr. Iftach Haitner; Dr. Benny Applebaum; Dr. Amos Fiat; Dr. Eran Tromer

Project Description:

This research studies essential aspects of the security, economy and policy implications of Bitcoin like digital currencies. Via the perspectives of cryptography, distributed computing, computer engineering and algorithmic game theory, the investigators aim to improve understanding, identify flaws and create new systems that serve society better in functionality and robustness. They are implementing a broad investigation of these issues, using their expertise in cryptography, computer engineering and Algorithmic Game Theory. They are pursuing previously unaddressed issues in the context of digital currency, such as

National fiscal and regulatory policies and their adaptation/interaction with distributed digital currencies, which will be pursued in collaboration with experts in economics and policy. They aim to deliver topnotch scientific publications and prototype implementations. Additionally, they aim to bolster research and education on digital currencies, security in decentralized systems in general and the requisite technical tools, by training graduate students and conducting workshops.

Securing Servers and Endpoints using Software Guard Extensions

Principal Investigators:

Prof. Sivan A. Toledo; Dr.. Eran Tromer

Project Description:

This research project addresses three crucial aspects of using SGX to secure servers and endpoints in such applications: analyzing the security of SGX itself; enabling SGX applications and integration with complementary approaches. In summary, the research will enable effective and rigorous use of the soon-to-be-ubiquitous SGX hardware, in the service of numerous applications that require trust in platforms.

Shocks to and Security in the Bitcoin Ecosystem: An Interdisciplinary Approach

Principal Investigators: Prof. Neil Gandal; Dr. Tyler Moore

Project Description:

This research includes the following key topics: the optimal resource allocation for protecting a network and the recent rise in digital currencies. The latter, which was led by the introduction of Bitcoin in 2009, creates an opportunity to measure information security risk in a way that has often not been possible in other contexts. Digital currencies (or cryptocurrencies) aspire to compete against other online payment methods such as credit/debit cards and PayPal, as well as serve as an alternative store of value. They have been designed with transparency in mind, which creates an opportunity to quantify risks better. While Bitcoin's design provides some safeguards against `counterfeiting' of the currency, in practice, the ecosystem is vulnerable to thefts by cybercriminals, frequently targeting intermediaries such as wallets or exchanges.

Smart Cities Cyber Security (SCCS)

Principal Investigators: Prof. Michael Birnhack; Prof. Issi Rosen-Zvi; Dr. Tali Hatuka

Project Description:

A theoretical and empirical study is being conducted, taking Israeli cities as a case study. Several Israeli cities take a leading role in developing Smart City, making them ideal candidates for initial research. The goal is to offer a multi-faceted toolkit for the optimal design of cyber systems for smart cities in Israel. This is a broad goal and it is impossible to cover all aspects of SCCS. Hence, the investigators are focusing on four interrelated dimensions, which they think are cornerstones of a viable SCCS: planning, technology, local governance and privacy. The analysis is being conducted separately and jointly, so as to explore the intersections between these dimensions. The research is creating a set of tools for policy-makers and municipalities in the process of developing a smart city.

Understanding IP Hijack Events

Principal Investigator: Prof. Yuval Shavitt

Project Description:

Surprisingly, a large-scale analysis of hijack events that will enable security system designers to understand this risk has never been published. In this project, hijack events are analyzed over time and active monitoring is compared with BGP based detection, specifically:

1. Building a BGP analysis tool improving previous published techniques; identifying hijack events using data from RouteViews, RIPE and others and analyzing hijack events to better understand their duration, target types, time of day, distance, etc.
2. Building a traceroute analysis tool to improve previously published techniques; identifying hijack events using data from at least two companies that already agreed to share data wand based on data from the DIMES project at TAU; analyzing the hijack events as above.
3. Comparing the two methods by identifying areas covered by both. Investigators expect to find hijack events that are not seen by BGP and are attempting to understand the technique used for the hijack. They are also using active monitoring to check if the hijack at the BGP level always results in packets following the new route.

Ultralong Fiber Laser for Secure Communications

Principal Investigator: Dr. Jacob Scheuer

Project Description:

The main objectives of this exploratory program are to investigate the resilience of a certain scheme to a variety of active attacks and to obtain quantitative metrics regarding information about the key that might be obtained by a potential adversary. The research includes both theoretical and experimental efforts to study the system's resilience to eavesdropping and for developing appropriate countermeasures.

Violence and the (Social) Construction of Cyber Deterrence

Principal Investigator: Dr. Amir Lupovici

Project Description:

The proposed research, which aims to yield a book-length manuscript, focuses on practices of cyber deterrence by exploring them in five countries—the US, Israel, Turkey, China and Russia—between the years 1999-2014. The project seeks to answer two main questions: 1) to what extent and how have these countries adopted a cyber deterrence strategy? 2) Is cyber deterrence an effective strategy, that is, does cyber deterrence affect cyber-attacks, and if so, how?

What's the Value of Bug Bounty Programs? Bug Bounty

Principal Investigator: Ms. Keren Elazari

Project Description:

The Vulnerability Rewards program, better known as Bug Bounty (BB) programs, are frameworks that allow companies to reward individual hackers for discovering and disclosing security and privacy breaches in the most popular sites in the world. To date, Facebook has paid hackers from around the world more than $2 million in rewards for their discoveries of bugs through its Bug Bounty program. Almost every major technology firm operates a similar framework. PayPal, Yahoo, Samsung, Twitter, Microsoft, Google are just a few familiar names among the hundreds of global companies that operate the Bug Bounty program in order to offer incentives to independent hackers and security researchers who report code-based weaknesses or breaches. The first BB plan was established for the browser Netscape in 1995. Today, 20 years later, ground-breaking research being conducted in the US found that Mozilla's BB program is one of the most cost effective tools for identifying weaknesses in software and security issues.

115 Principle Investigators in Blavatnik ICRC

Principal Investigator (PI) refers to the holder of an independent grant administered by a university and the lead researcher for the grant project. Each Blavatnik ICRC grant is awarded to the PI or PIs, at least one of which is TAU Faculty. In exploratory grants, persons who are not faculty are eligible to serve as PI, with a declaration of support by a TAU faculty. Blavatnik ICRC has **115** Principle Investigators.

List of Blavatnik ICRC Principle Investigators

Name	Affiliation		Country
Adam Morrison	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Adi Akavia	Haifa University	Computer Science	Israel
Alon Rosen	IDC	Efi Arazi School of Computer Science	Israel
Amir Averbuch	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Amir Globerson	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Amir Lupovici	TAU	Gershon H. Gordon Faculty of Social Sciences, Political Science	Israel
Amnon Ta- Shma	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Amos Fiat	TAU	Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Anat Bremler- Barr	IDC	Efi Arazi School of Computer Science	Israel
Anat Cohen	TAU	Lester and Sally Entin Faculty of Humanities, School of Education	Israel
Asher Tishler	TAU	Coller School of Management	Israel
Assaf Schuster	Technion	Computer Science Department & Joseph and Sadie Danciger Chair in Engineering	Israel
Aurojit Panda	New York University	Computer Science Department	USA
AviramZrahia	Corporate	Juniper LTD	Israel
Avishai Wool	TAU	Iby and Aladar Fleischman Faculty of Engineering, School of Electrical Engineering	Israel
Avner Levin	Ryerson University	Ted Rogers School of Management, Law & Business Department	Canada
Ayala Arad	TAU	Coller School of Management	Israel
Ayelet Gneezy	University of California, San Diego	Rady School of Management Associate Professor Of Marketing	USA

Name	Affiliation		Country
Benny Applebaum	TAU	Iby and Aladar Fleischman Faculty of Engineering	Israel
Benny Chor	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Bo An	Nanyang Technological University	School of Computer Science and Engineering Nanyang; Assistant Chair (Innovation)	Singapore
Chen Pundak	TAU	Coller School of Management	Israel
Dan Halperin	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Dan Tsafrir	Technion	Computer Science Department	Israel
Daniel Deutsch	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
David G. Schwartz	Bar Ilan University	Graduate School of Business Administration, Information Systems	Israel
David Horn	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Raymond and Beverly Sackler School of Physics and Astronomy	Israel
David Lo	Singapore Management University	School of Information Systems, Associate Professor of Information Systems	Singapore
Deborah Housen-Couriel	Advocate		Israel
Deganit Paikowsky	TAU	Gershon H. Gordon Faculty of Social Sciences	Israel
Dikla Perez	Bar Ilan University	Graduate School of Business Administration (Visiting)	Israel
Dino Levy	TAU	Coller School of Management, Neuroeconomics and Neuromarketing lab at the Marketing Department and Sagol School of Neuroscience	Israel
Dmitry Adamsky	IDC	Lauder School of Government	Israel
Dov Te'eni	TAU	Coller School of Management, Information Systems	Israel
Eli Amir	TAU	Coller School of Management, Accounting	Israel
Eli Brosh	Corporate	Canary Connect Ltd.	Israel
Eran Toch	TAU	Iby and Aladar Fleischman Faculty of Engineering, Industrial Engineering	Israel
Eran Tromer	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Erez Shmueli	TAU	Iby and Aladar Fleischman Faculty of Engineering, Industrial Engineering	Israel

Name	Affiliation		Country
Erran Carmel	American University	Kogod School of Business	USA
Gabi Shugul	Corporate	Astronautics C.A. Ltd	Israel
Gal Oetsreicher-Singer	TAU	Coller School of Management	Israel
Gal Sheppes	TAU	Gershon H. Gordon Faculty of Social Sciences, Clinical Psychology	Israel
Galia Rahav	TAU	Sackler Faculty of Medicine, School of Continuing Medical Education and Sheba Medical Center, Clinical Departments	Israel
Gao Debin	Singapore Management University	School of Information Systems	Singapore
George Westerman	MIT	Initiative on the Digital Economy	USA
Gil Baram	TAU	Gershon H. Gordon Faculty of Social Sciences, Department of Political Science	Israel
Gil Zussman	Columbia University	Electrical Engineering	USA
Haim Wismonski	Ministry of Justice	Israeli State Attorney's Office	Israel
Hanoch Levy	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
HyoDuk Shin	University of California, San Diego	Rady School of Management	USA
Iftach Haitner	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Ina Weiner	TAU	Gershon H. Gordon Faculty of Social Sciences, Psychology	Israel
Inbal Yahav-Shenberger	Bar Ilan University	Graduate School of Business Administration	Israel
Irad Ben-Gal	TAU	Iby and Aladar Fleischman Faculty of Engineering	Israel
Iris Shahar	Sheba Medical Center	Gertner Institute for Health Policy and Epidemiology	Israel
Isaac Ben Israel	TAU	Gershon H. Gordon Faculty of Social Sciences	Israel
Issi Rosen-Zvi	TAU	Buchmann Faculty of Law	Israel
Itzhak Benenson	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Geography and Human Environment	Israel
Itzhak Omer	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Geography and Human Environment	Israel
Jacob Goldenberg	IDC	Arison School of Business – Marketing	Israel
Jacob Scheuer	TAU	Iby and Aladar Fleischman Faculty of Engineering	Israel

Name	Affiliation		Country
Joachim Meyer	TAU	Iby and Aladar Fleischman Faculty of Engineering, Industrial Engineering	Israel
Keren Elazari	Corporate		Israel
Leonid Lev	Corporate	Israel Electric Company	Israel
Lior Tabansky	TAU	Gershon H. Gordon Faculty of Social Sciences	Israel
Lior Wolf	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Liu Yang	Nanyang Technological University	School of Computer Science and Engineering, Division of Software and Information Systems (SIS),	Singapore
Margarita Jaitner	Swedish Defence College		Sweden
Marie Vasek	University of New Mexico	Computer Science	USA
Matan Gavish	Stanford University	Department of Statistics	USA
Maytal Saar-Tsechansky	University of Texas, Austin	McCombs School of Business	USA
Metsada Pasmanik Chor	TAU	George S. Wise Faculty of Life Sciences, Bioinformatics	Israel
Michael Birnhack	TAU	Buchmann Faculty of Law	Israel
Mooly Sagiv	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Nadav Amit	Technion	Computer Science Department & VMware Research Group, Palo Alto, CA	USA
Nahum Kiryati	TAU	Iby and Aladar Fleischman Faculty of Engineering, Electrical Engineering	Israel
Neil Gandal	TAU	Eitan Berglas School of Economics	Israel
Noam Rinetzky	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Noam Shamir	TAU	Coller School of Management	Israel
Oded Maimon	TAU	Iby and Aladar Fleischman Faculty of Engineering, Industrial Engineering	Israel
Ohad Barzilay	TAU	Coller School of Management	Israel
Or Rabinowitz	Hebrew University of Jerusalem	Department of International Relations	Israel
Raazesh Sainudiin	Uppsula University	Mathematics Matematiska institutionen	Sweden
Raz Tikochinski	Corporate	Astronautics C.A. Ltd	Israel
Robert Deng	Singapore Management University	School of Information Systems, Professor of Cybersecurity; Deputy Dean, Faculty & Research Director	Singapore
Roey Tzezana	Brown University		USA

Name	Affiliation		Country
RonenAvraham	TAU	Buchmann Faculty of Law	Israel
RonenTalmon	Technion	Viterbi Faculty of Electrical Engineering	Israel
Roy Luria	TAU	Lester and Sally Entin Faculty of Humanities, School of Education	Israel
Roy Zuckerman	TAU	Coller School of Management	Israel
Sam Ransbotham	Boston College	Department of Information Systems	USA
Shachar Reichman	TAU	Coller School of Management	
Shahar Maoz	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Shai Levi	TAU	Coller School of Management	
Shaun Shuxun Wang	Nanyang Technological University	Nanyang Business School, Division of Banking & Finance	Singapore
Shay Gueron	Haifa University		
Mary Ho Shuyuan	Florida State University	College of Communication & Information	USA
Sivan A. Toledo	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Sonia Roccas	Open University	Psychology	Israel
Stefan Penczynski	Mannheim University	Department of Economics	Germany
Tal Soffer	TAU	Lester and Sally Entin Faculty of Humanities, School of Education	Israel
Tali Hatuka	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Geography	Israel
Tang Qian	Singapore Management University	School of Information Systems	Singapore
Tomer Geva	TAU	Coller School of Management	Israel
Tova Milo	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Tyler Moore	Southern Methodist University	Tandy School of Computer Science	USA
Udi Sommer	TAU	Gershon H. Gordon Faculty of Social Sciences, Department of Political Science	Israel
Wang Qiuhong	Singapore Management University	Assistant Professor of Information Systems	Singapore
Yael Hanein	TAU	Iby and Aladar Fleischman Faculty of Engineering, Electrical Engineering & NANO center	Israel

Name	Affiliation		Country
Yael Steinhart	TAU	Coller School of Management, Marketing Department	Israel
Yehuda Afek	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Yossi Azar	TAU	Raymond and Beverly Sackler Faculty of Exact Sciences, Blavatnik School of Computer Science	Israel
Yuval Shavitt	TAU	Iby and Aladar Fleischman Faculty of Engineering, Electrical Engineering	Israel
Zohar Yakhini	IDC	Efi Arazi School of Computer Science	Israel

BLAVATNIK ICRC ACADEMIC FELLOWS & VISITORS, 2018

In 2018, Blavatnik ICRC hosted sixty-three Academic Fellows & Visitors, which came to perform independent research, participate in scientific conferences, and educate young scientists.

The list does not include dozens of scientific visits performed by the Blavatnik ICRC PIs within their respective research programs.

Academic Fellows & Visitors, 2018

Title	Name	Affiliation
Mr.	Adam Conner	Resident Fellow at the Institute of Politics (IOP) at Harvard University
Dr.	Adam Segal	Lipman Chair in emerging technologies and national security and director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations (CFR)
Dr.	Adi Akavia	Director and founder of the Cybersecurity Research Institute at the Academic College of Tel Aviv Jaffa
Prof.	Alessandro Chiesa	Computer Science at UC Berkeley
Dr.	Allison Breton Bishop	Assistant Professor of computer science at Columbia University
Prof.	Andrew Yao	Tsinghua University, Beijing
Prof.	Ari Ezra Waldman	Professor of Law and the Director of the Innovation Center for Law and Technology at NYU
Prof.	Ari Shamiss	CEO of Assuta Medical Centers
Prof.	Avi Wigderson	Institute for Advanced Study (IAS), Princeton University
Adv.	Benjamin Ang Cheng Koon	Senior Fellow in the Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University. The fellowship was 4 weeks in length, from November 2018
Prof.	Boaz Barak	Harvard University
Dr.	Bruce Schneier	Fellow and Lecturer, Harvard Kennedy School
Mr.	Cameron Kerry	Visiting Fellow in Governance Studies and the Center for Technology Innovation at Brookings Institute
Prof.	Chester Dominic Rebeiro	Assistant Professor at the Indian Instituted of Technology, Madras
Prof.	Chris C. Demchak	Grace M. Hopper Professor & Chair of Cyber Security and Director, Center for Cyber Conflict Studies (C3S), Strategic and Operational Research Department, U.S. Naval War College
Dr.	Christoph Peylo	Global Head of Bosch Center for Artificial Intelligence (BCAI)
Prof.	Christos H. Papadimitriou	Columbia University
Dr.	Dor Minzer	Princeton University
Prof.	Elchanan Mossel	Massachusetts Institute of Technology (MIT)
Prof.	Eli Ben Sasson	Technion – Israel Institute of Technology

Title	Name	Affiliation
Prof.	Eugene Kandel	Professor of Economics and Finance at the Hebrew University in Jerusalem
Dr.	Gabriela Zanfir	
Prof.	Gil Kalai	Hebrew University of Jerusalem
Dr.	Gilat Kol	Princeton University
Prof.	Guy Kindler	Hebrew University of Jerusalem
Prof.	Irit Dinur	The Weizmann Institute of Science
Prof.	Itamar Grotto	Public Health School of Ben-Gurion University in Israel
Dr.	Jaclyn Kerr	Postdoctoral Research Fellow at the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory and at the Center for International Security and Cooperation (CISAC) at Stanford University.
Dr.	James Andrew Lewis	Senior Fellow, The Center for Strategic and International Studies (CSIS)
Prof.	Jeff Jarvis	Tow-Knight Center for Entrepreneurial Journalism, CUNY Graduate School of Journalism
Prof.	Jian Li	Tsinghua University, Beijing
Prof.	Jonathan Mayer	Assistant Professor of Computer Science and Public Affairs, Princeton University
Prof.	Joseph S. Nye	University Distinguished Service Professor and former Dean of Harvard's Kennedy School of Government.
Mr.	Justin Lee Holmgren	Princeton University
Dr.	Karolina Mojzesowicz	Deputy Head, Unit of Data Protection, European Commission
Prof.	Katarina Adam	Department of Business Administration and Engineering, HTW Berlin
Dr.	Katarina Linck	
Prof.	Leonid Eidelman	President-elect, World Medical Association.
Dr.	Mariarosalba Angrisani	Vice-director of CeRITT (Research Centre on Innovation and Technology Transfer), and Vice-chief of the Technology Transfer Office (TTO) – both of the Federico II University of Naples
Prof.	Martin Libicki	Keyser Chair of Cybersecurity Studies at the U.S. Naval Academy
Dr.	Michael Sulmeyer	Belfer Center's Cyber Security Project Director at the Harvard Kennedy School
Dr.	Michael Zlatin	Rutgers University
Prof.	Moran Cerf	Professor of neuroscience (department of neurosurgery, LIJ) and business (Kellogg School of Management)
Prof.	Oded Regev	New York University (NYU)
Prof.	Oded Schwartz	Hebrew University of Jerusalem
Prof.	Omer Tene	Associate Professor at the College of Management School of Law
Dr.	Osnat Levtzion-Korach	Director-General of Shamir Medical center
Dr.	Paul Cornish	Associate Director of Oxford University's Global Cyber Security Capacity Centre.

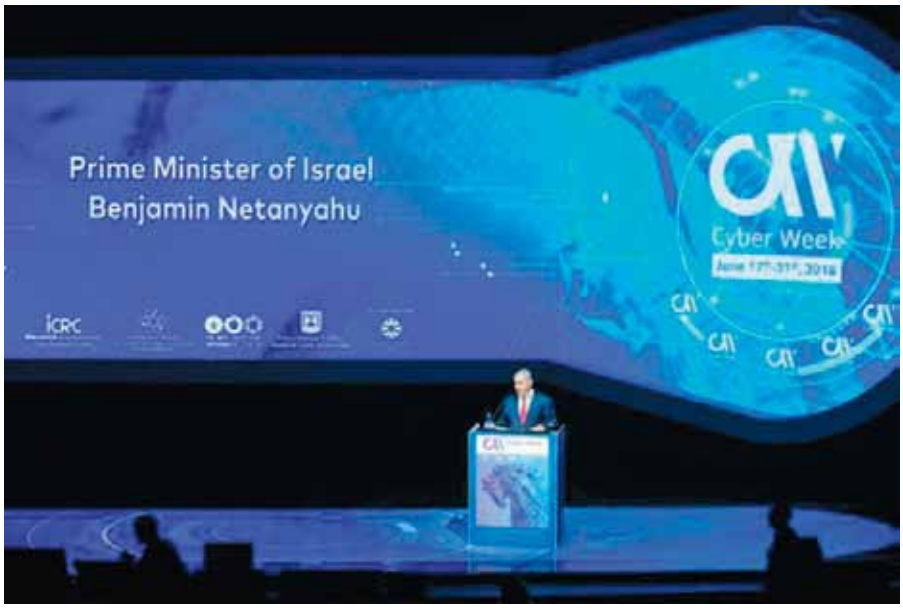
Title	Name	Affiliation
Dr.	Peter J. Fitzgerald	Director of the Center for Cardiovascular Technology and Director of the Cardiovascular Core Analysis Laboratory (CCAL) at Stanford University Medical School.
Prof.	Rafael Beyar	Director, Rambam Health Care CampusProfessor of Medicine and Biomedical Engineering, Technion.
Prof.	Raffaele Marchetti	Department of Political Science and the School of Government of Libera Università Internazionale degli Studi Sociali "Guido Carli" (LUISS)
Prof.	Ran Raz	Princeton University
Prof.	Ronitt Rubinfeld	Massachusetts Institute of Technology (MIT)
Prof.	Ronni Gamzu	CEO, The Tel Aviv Sourasky Medical Center
Prof.	Sandeep Shukla	Head of the Department of Computer Science and Engineering Department at the Indian Institute of Technology Kanpur
Prof.	Satoru Tezuka	Project Professor, Graduate School of Media and Governance, and Director, Cyber Security Research Center, Keio University
Prof.	Shafi Goldwasser	Simons Institute for the Theory of Computing, UC Berkeley
Prof.	Steven Bellovin	Computer Science department at Columbia University
Dr.	Tanya Filer	Head, Digital State Project at the Bennett Institute for Public Policy, University of Cambridge (visited as the 2018 UK-Israel British Council fellow, awarded for cyber research). The fellowship was 20 weeks in length, from May 2018.
Dr.	Tushant Mittal	University of Chicago
Dr.	V.S. Subrahmanian	Distinguished Professor in Cybersecurity, Technology, and Society and Director of the Institute for Security, Technology, and Society at Dartmouth College
Prof.	Vitaly Shmatikov	Computer Science at Cornell Tech and Cornell University
Dr.	Zekeriya Erkin	Professor, Cyber Security Group, Delft University of Technology

CYBER WEEK 2018

The eighth annual Cyber Week 2018 international cybersecurity conference we held on June 17-21, 2018 was the biggest and most diverse yet.

Cyber Week 2018 full original agenda is attached as Appendix A.

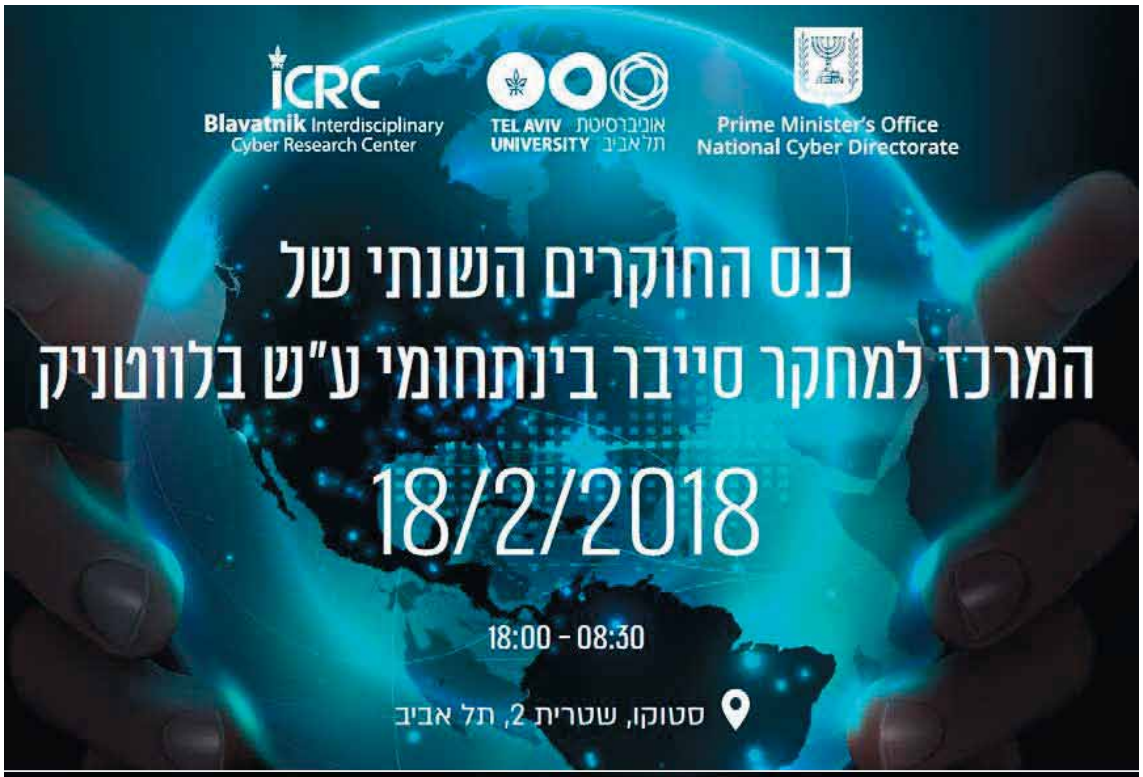
Cyber Week 2018 press kit is attached as Appendix B.



The original Cyber Week 2018 website

The Cyber Week 2018 Album is online

BLAVATNIK ICRC RESEARCH RETREAT 18/02/2018



דברי פתיחה: פרופ' איציק בן ישראל, ראש המרכז למחקר סייבר בינתחומי ע"ש בלווטניק ויו"ר סדנת יובל נאמן למדע טכנולוגיה וביטחון

גילי דרוב היישטיין, מנהלת המרכז למחקר סייבר בינתחומי ע"ש בלווטניק

סיכום שנתי: מדדי ביצוע מרכזיים

ד"ר יניב הראל, ראש אסטרטגיית המחקר, המרכז למחקר סייבר בינתחומי ע"ש בלווטניק

ליאור טבנסקי, ראש פיתוח מחקר, המרכז למחקר סייבר בינתחומי ע"ש בלווטניק

מושב ראשון

פרופ' ליאור וולף, הפקולטה למדעים מדויקים

Compilation Integrity Assurance through Deep Code Alignment

פרופ' אבישי וול, הפקולטה להנדסה

Avionic Bus Cyber Attack Identification

פרופ' יעל שטיינהרט, הפקולטה לניהול

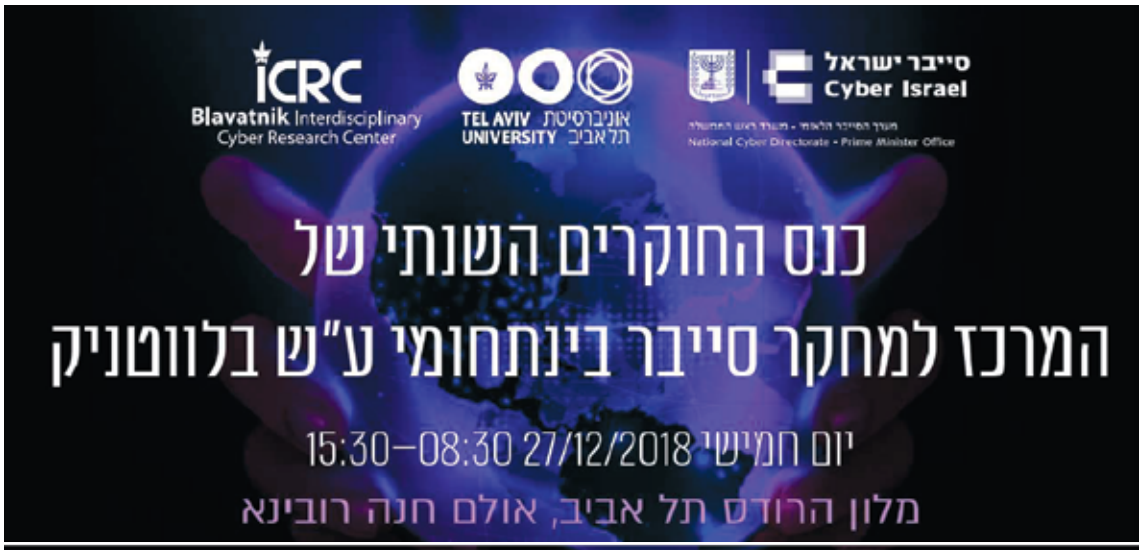
The Selfish and Caring of Sharing: Exploring the Reasons and Personal Outcomes of Public Shaming

פרופ' דוד הורן, הפקולטה למדעים מדוייקים

Adapting QC and MEC algorithms to Anomaly Detection in Big Data

הפסקת קפה

BLAVATNIK ICRC RESEARCH RETREAT 21/12/2018



דברי פתיחה

פרופ' איציק בן ישראל, ראש המרכז למחקר סייבר בינתחומי ע"ש בלווטניק וויו"ר סדנת יובל נאמן למדע טכנולוגיה וביטחון

גילי דרוב היישטיין, מנהלת המרכז למחקר סייבר בינתחומי ע"ש בלווטניק

עינן ליכטרמן, ראש תחום בכיר מו"פ וטכנולוגיות, אגף אסטרטגיה והתעצמות, מערך הסייבר הלאומי, משרד ראש הממשלה

הצגת מחקרים: מושב ראשון

Detecting Cryptocurrency Scams and Measuring Cryptocurrency Quality / Prof. Neil Gandal, Berglas School of Economics

Reconciling Cyber-Security Research with Privacy Law: The Video Analytics and Medical Image Analysis Examples / Prof. Nahum Kiryati, School of Electrical Engineering

A Novel Technology for Detecting Deceptive Behavior / Dr. Dino Levy, Coller School of Management

Evolving Cyber-threats and Countermeasures: Mathematical, Behavioral and Legal Perspectives / Prof. Joachim Meyer & Omer Peled, Iby and Aladar Fleischman Faculty of Engineering

הפסקת קפה

הצגת מחקרים: מושב שני

The Dynamics and Geography of the Cybersecurity Industry / Prof. Tali Hatuka, Department of Geography and Human Environment

Mobile Phone Data for Society and Privacy for the Individual: From the Conflict to a Synergy in Transport Flows Analysis / Prof. Itzhak Benenson, Faculty of Social Sciences

The Deterrence Strategies of Non-States Cyber Actors / Dr. Amir Lupovici, School of Political Science, Government and International Affairs

Advanced Attacks against Internet Security Protocols / Prof. Yuval Shavitt, Iby and Aladar Fleischman Faculty of Engineering

Lior Tabansky, Head of Research Development, Blavatnik Interdisciplinary Cyber Research Center

הצגת מחקרים: מושב שלישי

Secure Shared Learning in Healthcare: Inference of Hospital Infection Risks / Dr. Adi Akavia, Department of Electrical Engineering and Computer Science, Dr. Iris Shahar, Gertner Institute

Non-Public Hacks / Dr. Roy Zuckerman, Coller School of Management

Towards Higher Accuracy of Behavioral Big Data Analysis: Using Qualitatively Augmented Hierarchical Classifier Algorithms / Prof. David G. Schwartz, Graduate School of Business, Bar-Ilan University

Memory Access Safety-Checking Tools for Programs that Share Memory with Devices / Dr. Adam Morrison, School of Computer Science

דיון וסיכום

Application Security Israel Conference (OWASP APPSEC-IL)

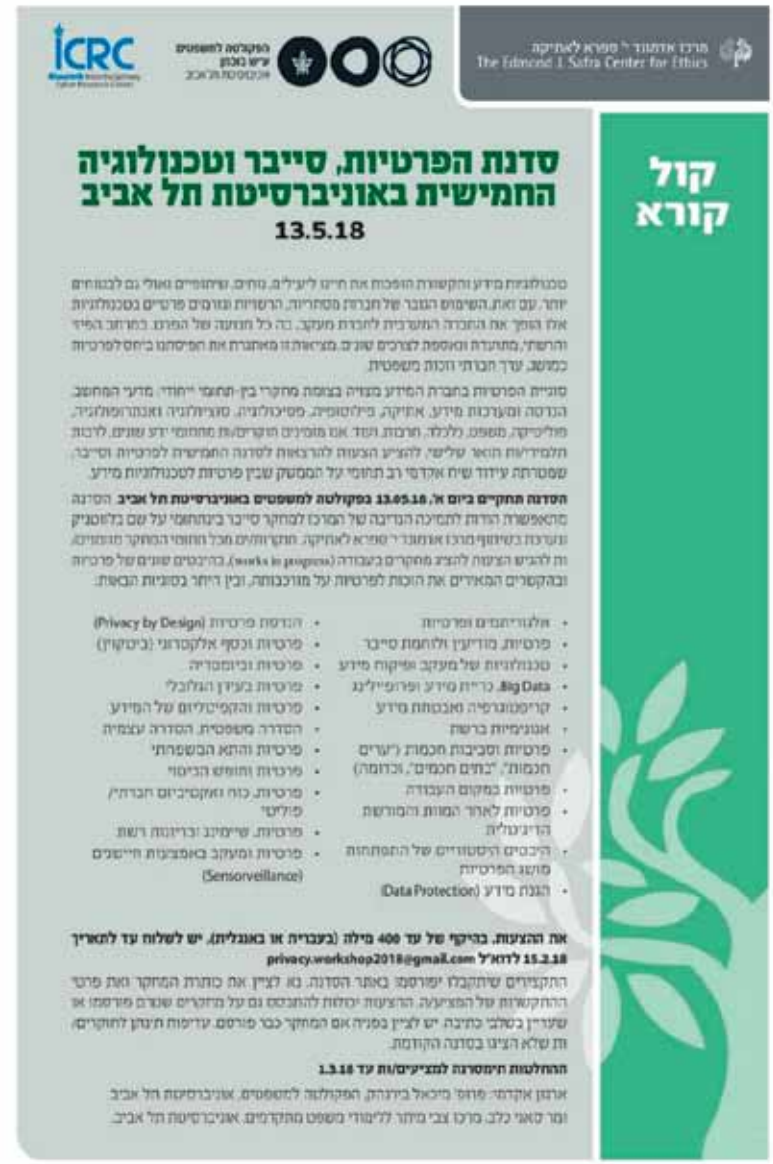
We at Blavatnik ICRC know firsthand a gap exists between academia and industry in cyber. We make the most of our deep ties with all stakeholders to bridge the gaps. This year, we co-hosted the annual OWASP AppSec Israel Conference which took place at Tel Aviv University.

The Open Web Application Security Project (OWASP) aims to be the thriving global community, which drives visibility and evolution in the safety and security of the world's software. OWASP is an open-source, not-for-profit application security organization, made up of corporations, educational organizations, and individuals, from around the world. OWASP boasts 46,000+ individual members, more than 65 organizational supporters, and numerous academic supporters. Providing free, vendor-neutral, practical, cost-effective application security guidance, the OWASP Foundation is the de-facto standards body for web application security, used by developers and organizations globally.

AppSec Israel 2018 had three lecture tracks, some hands-on workshops, and a Capture the Flag Competition. Over 650 attendees came to TAU's campus for OWASP APPSEC-IL. See the agenda online: https://2018.appsecil.org/Agenda

The Fifth Privacy, Cyber and Technology Workshop

Together with the Buchmann Faculty of Law, we held the Fifth Privacy, Cyber and Technology Workshop. As usual, the participants were selected through a call for papers. This time, three Blavatnik ICRC PIs were accepted. The program is available at



INSTITUTIONALIZED INTERNATIONAL RESEARCH COLLABORATIONS

The Blavatnik ICRC has already entered formal MoUs with several academic institutions, as well as agreements with several academic institutions and organizations worldwide. We have been transforming these into action.

Tata Consultancy Services (Tcs) Funding for Blavatnik ICRC Research

Tata Consultancy Services (TCS) is a multinational information technology (IT) service and consulting company. Part of India's TATA conglomerate, TCS is the world's second largest IT services provider, and is committed to innovation through its strong Co-Innovation Labs network.

Reaffirming the excellent research quality of the Blavatnik Interdisciplinary Cyber Research Center, TCS together with Ramot TTC launched a fund of several thousand US Dollars dedicated for cybersecurity research by Tel Aviv University faculty.

Prof. Avishai Wool, Deputy Director of the Blavatnik ICRC, Professor at the School of Electrical Engineering, Iby and Aladar Fleischman Faculty of Engineering, TAU and Director of the Cryptography and Network Security Lab, has been appointed to lead this activity. The Call for Proposals has received twelve submissions, which have been reviewed during Q3-Q4 2018.

The dedicated committee comprised of four TCS and three TAU representatives will reach funding decisions in Q1 2019.

As part of the working partnership, a delegation led by Prof. Joseph Klafter (President, TAU) and Prof. Isaac Ben-Israel, travelled to India in 2018, to participate in a joint seminar.

National Research Foundation (Singapore) Funding Joint Research with Blavatnik ICRC

The NRF-TAU collaboration program was launched in May 2016 to support joint research projects through an interdisciplinary approach with an emphasis on cybersecurity for Smart Nation and Internet of Things, behavioral and social science approaches to cybersecurity, and policy and governance aspects of cybersecurity.

NRF awarded $ 1,199,544 in funding to four joint research projects

1. Improving Cybersecurity through Optimal Policy Design and Human Behavior Modelling

Principal Investigators:

Lead Principal Investigator: Assistant Professor Bo An, School of Computer Science and Engineering, Nanyang Technological University

Co-Principal Investigator: Assistant Professor Liu Yang, School of Computer Science and Engineering, Nanyang Technological University

Collaborator from Tel Aviv University: Professor Joachim Meyer, Department of Industrial Engineering, Iby and Aladar Fleischman Faculty of Engineering

This project aims to design efficient policies for the government to reduce cyber-attacks through analyzing the interactions between different parties involved in the cyber ecosystem. This includes:

- Governments, who build the fundamental infrastructures and issue policies and laws to regulate the cyber activities;
- Service providers, who provide various cyber services, such as online banking, online security insurance, cloud computing, etc.;
- Users, who are the majority of the participants in the ecosystem; and
- Cyber attackers who seek to cause damages to both service providers and users, for their own benefit.

2. Deterring Cybersecurity Threats through Internet Topology, Law Enforcement and Technical Mitigation

Principal Investigators:

Lead Principal Investigator: Assistant Professor Wang Qiuhong, School of Information Systems, Singapore Management University

Co-Principal Investigator: Assistant Professor Tang Qian, School of Information Systems, Singapore Management University

Co-Principal Investigator: Professor Robert Deng, School of Information Systems, Singapore Management University

Collaborators from Tel Aviv University:

Professor Yuval Shavitt, School of Electrical Engineering, Iby and Aladar Fleischman Faculty of Engineering,

Mr. Lior Tabansky, Department of Political Science, Gershon H. Gordon Faculty of Social Sciences

This project addresses the two key questions of how we can characterize the interdependency of cyber-attacks and how we can achieve a balance between openness and security, when implementing international enforcement and technology information sharing to counter cyber-attacks.

The research team will model how cyber-attacks across regions, are interdependent by linking it back to the underlying Internet topology. They will also quantify the relative effectiveness of domestic law versus international law in deterring cyber-attacks, and evaluate how the extent of information shared by cybersecurity emergency response agencies alleviates cybersecurity threats.

3. Safety and Privacy of Smart City Mobile Applications through Model Inference

Principal Investigators:

Lead Principal Investigator: Associate Professor David Lo, School of Information Systems, Singapore Management University

Co-Principal Investigator: Associate Professor Gao Debin, School of Information Systems, Singapore Management University

Collaborators from Tel Aviv University:

Dr. Shahar Maoz, Blavatnik School of Computer Science

Dr. Eran Toch, Department of Industrial Engineering, Iby and Aladar Fleischman Faculty of Engineering

Dr. Eran Tromer, Blavatnik School of Computer Science

This project aims to protect the safety and privacy of people who use mobile applications to access smart city services.

The project will design a system that detects anomalous and potentially harmful behaviors in apps and create suitable alerts. By creating a model that captures the characteristics of an app's normal behavior, it can help to detect violations during runtime, summarize the risk in an informative manner, and give users the opportunity to disallow or approve it.

There will also be user interaction models for different users, such as power users, senior citizens and children.

4. Quantification of Cyber Risk

Principal Investigator: Lead Principal Investigator: Professor Shaun Wang, Division of Banking & Finance, Nanyang Business School, Nanyang Technological University

Collaborators from Tel Aviv University:

Professor Asher Tishler, Coller School of Management

Dr. Ohad Barzilay, Coller School of Management

Mr. Amitai Gilad, Coller School of Management

This project will facilitate new areas of research in cyber risk, security and insurance at Nanyang Technological University and will also recommend policies to the Singapore government on advanced cyber risk protection and prevention. It will combine the technological, strategic and behavioral aspects of cybersecurity together to form an academic framework.

5. Blavatnik Icrc & European School of Management and Technology (Germany)

The European School of Management and Technology (ESMT) is a State-accredited private university-level business school with the right to grant PhDs. Founded in 2002 in Berlin by 25 leading German corporations and institutions, it is now rated among the world's best.

Its Digital Society Institute (DSI), is decidedly independent, inter-and transdisciplinary, intelligible and pragmatic and shows a strong emphasis on cyber security and digital privacy. It aggregates and develops basic research using methodological approaches and theories and combines them with an application-oriented and holistic viewpoint, thereby providing metrics and frameworks to measure, understand and predict the digital world, and to develop responsible strategies for our digital future.

Following deep mutual appreciation based on previous engagements of scholars, TAU ICRC and ESMT DSI a research collaboration came about. This year, we submitted a proposal to NATO SPS. However, the proposal did not win. To the best of our knowledge, this was due to political reasons: Turkey blocked NATO SPS funding to Israeli partners.

In 2018, three Blavatnik ICRC researchers delivered a Workshop "AI in Cybersecurity Technical, Strategic and Global Aspects" at their annual Digital Society Conference 2018: Empowering Ecosystems

Blavatnik ICRC & Cyberlab (Italy)

On July 20, 2015, TAU and The University of Modena and Reggio Emilia (UniMoRe), within the framework of the Italian Cyber Security National Lab, signed an agreement to create a new cooperation in the form of a joint cyber lab. The Cyber Lab was established in Italy, with the Department of Engineering, "Enzo Ferrari", at UniMoRe coordinating the activities.

Professor Sergio Ferrari, Deputy Rector of The University of Modena and Reggio Emilia and Prof. Joseph Klafter, President of TAU, as well as Prof. Aron Shai, the then rector of TAU, signed the agreement. This partnership came about following the joint declaration of the government of the Italian Republic and the government of the State of Israel, on Bilateral Cooperation on Cyber Space, which was signed in Rome, on December 2, 2013.

Since the signing of a Memorandum of Understanding in 2015, two of our researchers began working on various projects with the University of Modena. Lior Tabansky, launched a project with the university examining the policy aspects of cybersecurity and Prof. Avishai Wool, has been working with the University of Modena on his project related to automated cars.

In January 2017, as part of this cooperation, Prof. Marco Mayer, Adjunct Professor of Conflict and Peacebuilding at LUISS & Director of MA Intelligence and Security at Link Campus University, was invited by the center to deliver the keynote address at our conference on Politics and Cyber.

In recognition of the role the Blavatnik ICRC and Professor Ben Israel have played in strengthening the diplomatic ties between Italy and Israel in the field of cyber innovation, Professor Ben Israel was awarded an honorary knighthood during the 7th Annual International Cybersecurity Conference.

However, internal organizational issues in Italy will likely terminate this CyberLab, and instead, our counterparts in Italy, will erect a different and more effective framework.

Blavatnik ICRC & Confederation of Indian Industries (CII), India

Confederation of Indian Industries (CII) works to create and sustain an environment conducive to the development of India, partnering industry, Government, and civil society, through advisory and consultative processes. As such, their aim coincides with the focus of the Blavatnik ICRC. Israel has one of the greatest cyber capabilities in the world; India has one of the biggest software services field. This presents a great opportunity for both countries. In 2015, the Blavatnik ICRC and CII signed a Memorandum of Understanding.

In May 2018, representatives from TAU, were invited to participate in the Global Expo Services in Mombay.

In December 2018, representatives from TAU were invited to participate in the 11th India-Israel Forum hosted by CII. The event focused on a range of topics including Policy and smart cities. The event was a definite success and we look forward to hosting the 12th event in Israel in 2019.

The Blavatnik ICRC and CII worked together for many months to create the India-Israel Roundtable during Cyber Week 2018. The roundtable welcomed over 60 attendees of which 35 were part of the CII official delegation to the conference. The roundtable focused on "policy" and "from startups to marketplace" – important topics for both countries. We were privileged to have Ambassador Pavan Kapoor, the Indian Ambassador to Israel, at the event.

Blavatnik ICRC & Indian Institute of Technology, Kanpur (India)

The Ministries of Science in India and Israel awarded a joint research project between Professor Amir Averbuch (ICRC) and Professor Sandeep Shukla (IITK) with a grant in 2018.

IMPACT, OUTREACH AND ENGAGEMENT

The Blavatnik ICRC has worked hard to build an interdisciplinary scientific community. We at Blavatnik ICRC know firsthand that a gap between academic disciplines inhibits research progress. We leverage our deep ties with all stakeholders to bridge the gaps. Our researchers have been participating in many conferences abroad and sharing their insight and progress in scientific journals as well as popular media outlets.

Outstanding Global Research Impact

The high level of interdisciplinary research taking place at the Blavatnik ICRC has had a broad range of international impact; influencing worldwide legal policy, international media and public awareness. Below are two examples of such research:

"Price Manipulation in the Bitcoin Ecosystem"

The research "Shocks to and Security in the Bitcoin Ecosystem: An Interdisciplinary Approach" by Prof. Neil Gandal, funded by the Blavatnik ICRC in 2016, resulted in articles in influential economic and cybersecurity journals.

The Journal of Monetary Economics, a top journal in economics, recently published the paper *"Price Manipulation in the Bitcoin Ecosystem."* In the paper, Neil Gandal, JT Hamrick, Tyler Moore, and Tali Oberman identified and analyzed the impact of suspicious trading activity on the Mt. Gox Bitcoin currency exchange: approximately 600,000 bitcoins (BTC) valued at $188 million were fraudulently acquired. The USD- BTC exchange rate rose by an average of four percent on days when suspicious trades took place, compared to a slight decline on days without suspicious activity. Based on rigorous analysis with extensive robust checks, we concluded that the suspicious trading activity by the Mt. Gox exchange itself likely caused the unprecedented spike in the USD-BTC exchange rate in late 2013, when the rate jumped from around $150 to more than $1,000 in two months.

The paper has been well cited in the academic literature (it already has 57 Google citations) – and received coverage by the New York Times, Tech Crunch and many other leading media outlets.

More importantly, this is an example of academic research directly influencing policy in the real world. The *July 2018 U.S. Securities and Exchange Commission (SEC) rule to reject Bitcoin Exchange Traded Fund* (ETF) was based on the research conducted by Prof. Gandal and his team. The rejection of the proposal (submitted by Cameron and Tyler Winklevoss) was in part taken because concerns of possible price manipulation. In their recent order (Release No. 34-83723; File No. SR-BatsBZX-2016-30), the SEC remarked that *Gandal et. al, 2018* paper and several other academic studies "supplement the Commission's conclusion" that the proposers have not shown that Bitcoin markets are "resistant to manipulation." The SEC notes that they would have rejected the proposal even without these academic papers. Nevertheless, it is important that the SEC is using academic research as supplemental material.

This research demonstrates that there is concern about short-term pricing and, perhaps, liquidity issues associated with some exchanges. It shows that when markets are developing, the usual checks and balances that can be used to detect manipulation and other issues cannot be deployed due to a lack of longer time series data on 'normal' behavior.

Reference:

"Price Manipulation in the Bitcoin Ecosystem," 2018, (Neil Gandal, JT Hamrick, Tyler Moore, and Tali Oberman,) *Journal of Monetary Economics*, https://doi.org/10.1016/j.jmoneco.2017.12.004 .

Feder, Amir, Neil Gandal, J. T. Hamrick, and Tyler Moore. "The Impact of Ddos and Other Security Shocks on Bitcoin Currency Exchanges: Evidence from Mt. Gox." *Journal of Cybersecurity* 3, no. 2 (2017): 137-44. http://dx.doi.org/10.1093/cybsec/tyx012

"Advanced Attacks Against Internet Security Protocols"

The research "Shocks to and Security in the Bitcoin Ecosystem: An Interdisciplinary Approach" by Prof. Yuval Shavitt, funded by the Blavatnik ICRC in 2016, resulted in a joint interdisciplinary article on a topical policy issue.

Prof. Shavitt met Dr. Demchak at the Cyber Week conferences, and despite coming from different academic disciplines, they discovered a common research agenda.

Research conducted by Prof. Yuval Shavitt (Blavatnik ICRC) and Dr. Chris Demchak (US Naval College) showed how China Telecom seems to employ its distributed points of presence (PoPs) in western democracies' telecommunications systems to selectively redirect internet traffic through China. It also shows the observed routing paths, give a summary of how one hijacks parts of the internet by inserting these nodes, and outlines the major security implications.

Aside from influencing policy, the research article is making headlines worldwide. The article was downloaded 40,000 times in the first month, topping all other articles in Military Cyber Affairs journal combined. The authors first presented their research findings at the *Emerging Technologies in Great Power Competition* conference during *CYBERWEEK 2018*

We invite you to view the video of the talk.

The publication attracted worldwide attention among IT-security experts, defense professionals and public. Bruce Schneier, internationally renowned security technologist, quoted the article when blogged on "China's Hacking of the Border Gateway Protocol" and delivered the news to 250,000 subscribers. A ZDNet article dedicated to the research was titled China has been 'hijacking the vital internet backbone of western countries.' Ars Technica of WIRED Media Group also quoted the research in their "Strange snafu misroutes domestic US Internet traffic through China Telecom" piece.

Reference:

Demchak, Chris C, and Yuval Shavitt. "China's Maxim–Leave No Access Point Unexploited: The Hidden Story of China Telecom's Bgp Hijacking." *Military Cyber Affairs* 3, no. 1 (2018): 7. https://doi.org/10.5038/2378-0789.3.1.1050

Making headlines worldwide:

https://www.theregister.co.uk/2018/11/06/oracles_netwatchers_agree_china_telecom_is_a_repeat_bgp_offender/

https://nakedsecurity.sophos.com/2018/10/30/china-hijacking-internet-traffic-using-bgp-claim-researchers/

https://www.techspot.com/news/77129-researchers-discover-china-has-least-ten-pops-uses.html

https://www.hackerworldnews.com/china-hijacking-internet-traffic-using-bgp-claim-researchers/
https://boingboing.net/2018/10/26/bgp-pop-mitm.html

https://www.securityweek.com/china-telecom-constantly-misdirects internet-traffic

https://www.itnews.com.au/news/china-systematically-hijacks-internet-traffic-researchers-514537 https://threatpost.com/googles-g-suite-search-and-analytics-traffic-taken-down-in-hijacking/139060/

https://uk.reuters.com/article/uk-alphabet-disruption/nigerian-firm-takes-blame-for-routing-google-traffic-through- china-idUKKCN1NI2E9 "

https://venturebeat.com/2018/11/13/nigerian-telecom-fesses-up-to-routing-traffic-through-china/amp/

Australia: The Sydney Morning Herald How China diverts, then spies on Australia's internet traffic

Germany: Die WELT Für 74 Minuten kapert China das Google-Netz

Canada: The Globe and Mail China Telecom diverted internet traffic in U.S. and Canada, report finds

Finland: TIVI

Greece: https://katohika.gr/diethni/ti-megalyteri-kyvernoepithesi-stin-istoria-tis-dechtike-i-google/

Nigeria: https://engineersforum.com.ng/2018/11/14/russia-and-china-attack-google/

Czech: https://www.zive.cz/clanky/cina-mozna-roky-odposlouchava-podstatnou-cast-internetu/sc-3-a-195820/default.aspx

Switzerland: https://www.nzz.ch/digital/google-datenpakete-auf-abwegen-ld.1436550

UK: DailyMail

Reuters: Nigerian firm takes blame for routing Google traffic through China

"You can always claim that this is some kind of configuration error," said ***Shavitt****, who last month co-authored a paper alleging that the Chinese government had conducted a series of internet hijacks.* http://news.trust.org/item/20181113175316-80rgd/

Global Speaking Engagements, Media and Delegations

The Blavatnik ICRC receives several dozen delegations annually. The Director, Managing Director and the Head of Research Development, accommodates most visitors.

The Director, Professor Ben-Israel, is a frequent commentator, speaker at international conferences, academic institutions as well as at international cyber companies. The Head of Research Development leverages his participation in conferences and seminars around the world to promote the Blavatnik ICRC activity. Blavatnik ICRC takes the front stage in every both participate.

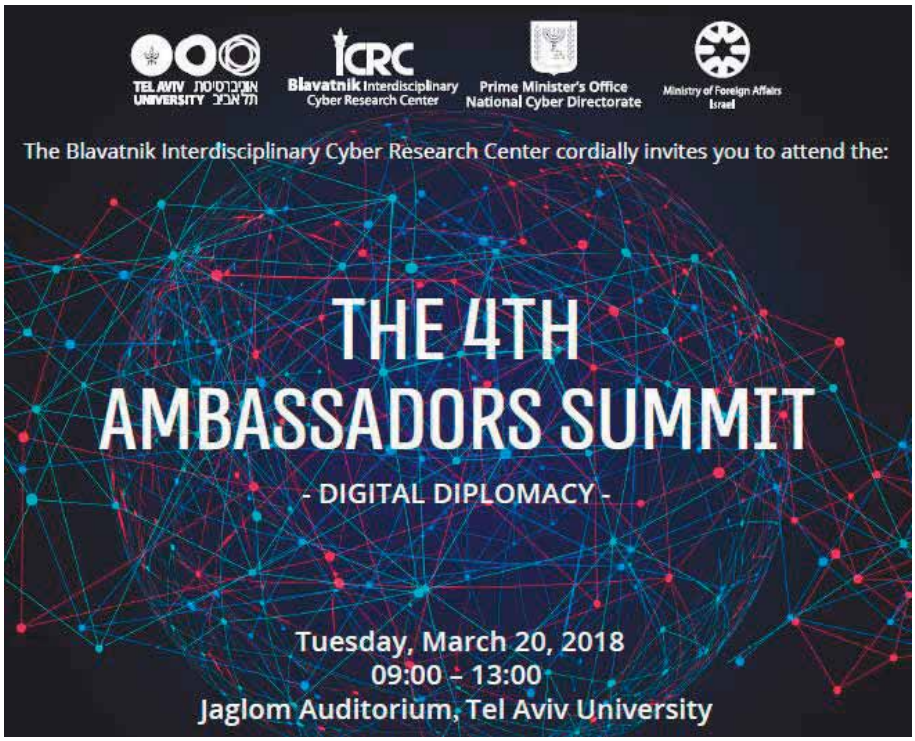
Global Speaking Engagements, 2018

Speaking Event Details	2018 Dates	Country
Lecture at the Israel Ministry of Foreign Affairs: "Technological Developments in Security"	January 15	Israel
Voice of America Interview with Michael Lipin	January 18	USA
Global Commission on the Stability of Cyberspace (GCSC)	January 23–25	Holland
The 13th Ilan Ramon International Space Conference	January 29–30	Israel
Global Space & Technology Convention 2018	January 31– February 2	Singapore

Speaking Event Details	2018 Dates	Country
Cybersecurity as Innovation: Israel's Experience. University Federico II, Naples	February 1	Italy
Airpower in Future Joint Operations – a Multi-Domain Battle. The Royal Norwegian Air Force Academy Annual Conference, Luftkrigsskolen 2018, Trondheim	February 6–8	Norway
Wall Street Journal Conference, San Francisco 2018	March 4–9	USA
Keio University, Tokyo	March 30 – April 2	Japan
The Future of Middle Eastern Cyber Warfare – Konrad-Adenauer-Stiftung Mediterranean Advisory Group, Jerusalem	April 26–27	Israel
Systemic Cyber Defense: Integrating Economics, Information, Innovation, and Operationalization Workshop. Center for Cyber Conflict Studies (C3S), US Naval War College, Newport RI,	May 1–2	USA
12th Asia-Pacific Program for Senior National Security Officers (APPSNO 2018)	May 6–11	Singapore
4th Global Exhibition on Services (GES), Cyber Resilience: Adaptive Line of Defense, Bombay Exhibition Centre, Mumbai	May 17	India
GLOBSEC 2018 Conference, Bratislava,	May 17–18	Slovakia
Cyber Security Summit, Tallinn	May 29	Estonia
MIT: Lecture to Students	June 2	USA
Israel Innovation and Safe Cities	June 5–6	France
The American Jewish Committee (AJC) Plenary, 2018	June 10–13	Israel
Civilizations of Knowledge Conference, 2018	June 10–11	Israel
ST Electronics Technology Seminar, 2018	June 27	Singapore
Processes of International Negotiation: New Diplomacy for New Types of Conflict, Hamburg,	July 2–3	Germany
Kommander Führungsunterstützung & Cyber Defence, Austria, Vienna,	July 4	Austria
Austrian Institute of Technology GmbH (AIT)	July 5	Austria
Innovation Day, Buenos Aires	July 5	Argentina
Digital Accelerator Tel Aviv	July 18	
S. Rajaratnam School of International Studies, Nanyang Technological University	July–August	Singapore
Bratislava	September 16–18	Slovakia
Singapore National Cybersecurity R&D Program International Advisory Panel (IAP)	September 17–19	Singapore

4th Annual Ambassadors' Summit

This annual event brings together cyber experts, ambassadors, international representatives and attaches for a riveting discussion. As part of the Center's cooperation with the Ministry of Foreign Affairs, we proudly hosted the 4th Ambassadors' Summit on March 20, 2018. Ambassadors and attaches came to TAU to learn from cyber experts and to join the discussion on global cybersecurity threats and the bilateral cooperation needed to strengthen the global ecosystem.



Opening Session

Maj. Gen. (Ret.) Prof. Isaac Ben Israel, Director, Blavatnik ICRC & Yuval Ne'eman Work shop for Science, Technology and Security at Tel Aviv University
Gili Drob-Heistein, Executive Director, Blavatnik Interdisciplinary Cyber Research Center
Iddo Moed [Moderator] - Cyber Security Coordinator, Ministry of Foreign Affairs
Yigal Una, Director General, National Cyber Directorate, Prime Minister's Office
Noam Katz, Senior Deputy Director General, Public Diplomacy, Ministry of Foreign Affairs

First Session

Global cyber politics
Brig. Gen. (Res.) Daniel "Danny" Bren, Former Commander of the Cyber Defensive Division of the IDF C4I Directorate

Possible traces of cyber-attacks on recent European elections
Prof. Yuval Shavitt, School of Electrical Engineering, Tel Aviv University

Between diplomacy and hostile influence: shades of cyber power
Lior Tabansky, Head of Research Development, the Blavatnik Interdisciplinary Cyber Re search Center, Tel Aviv University

The Diplomatic Arena: Developing counter narrative tools
Daniel Cohen, Researcher, The Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University

Coffee Break & Networking

Second Session

National Level Cyber Security
Esti Peshin, General Manager, Cyber Division, Israel Aerospace Industries

Blockchain and Digital Diplomatic Challenges
Jacob Mendel, General Manager, Cyber Security COE, Intel, Head of Industry Research Co operation, the Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University

The future of Cybersecurity education
Ophir Bear, CEO & Co-Founder, Cympire

Integrating Artificial Intelligence Into Cyber Security
Aviram Zrahia, Cyber Security Consulting Engineer, Juniper Networks, Researcher, the Blavatnik Interdisciplinary Cyber Research Center

We are looking forward to hosting the next Annual Ambassadors' Summit in Q1 2019.

Senior Cyber Forum

Blavatnik ICRC continued the engagement with a select group of senior stakeholders through our Senior Cyber Forum. Over one hundred leaders from business and public sectors take part in the trusted public-private partnership.

The October 29th Senior Cyber Forum meeting focused on the financial services sector.

MONDAY, OCTOBER 29TH, 2018, 09:00 -13:00
TEL AVIV UNIVERSITY, NAFTALI BUILDING, ROOM 527 (VENEZUELA HALL)

Executive Education Program: Effective Cybersecurity

Since 2017, we have been working to develop an Executive Education program. Such an offering serves our strategy to expand ties with the global stakeholders through outreach that adds value. We designed a modular offering that we tailor to each customer.

We partnered with the Lahav Executive Education Company at TAU's Coller School of Management. Lahav has developed and delivered state of the art programs for thousands of foreign and Israeli executives. In 2018, we successfully delivered the first Executive Education program to a group of 28 public sector managers from an Asian country.

See the opening sections of the program description:

Cybersecurity is a global, multifaceted, complex and rapidly morphing challenge. Managing it demands shared efforts by all stakeholders on the national and regional levels. Israel has proven outstanding cybersecurity abilities: world's most resilient critical infrastructure; groundbreaking technical innovation; world's second largest exporter of cybersecurity product and services, while attracting 15% of global private investment in cyber R&D. How did this small country, with its harsh environment become the "Start-up Nation" and a global science, technology and economic cyber powerhouse?

Rather than enjoying "unique abilities," Israel through her daily experiences, dares to make a broad range of policy decisions, investments and genuine inventions over the years throughout academia, business and government sectors. Over the years, a flourishing cyber ecosystem has developed in Israel, in which security agencies, academic research institutions, government agencies, and private companies aligned almost synergistically. This dynamic ecosystem drives recent cybersecurity advances.

Tel Aviv University is a pivotal element within the Israeli cyber ecosystem. TAU's Blavatnik Interdisciplinary Cyber Research Center (est. 2014) conducts over 60 cutting-edge research projects on diverse facets of cybersecurity, performed by 250 researchers, drawing on extensive intellectual networks within Israel and internationally. One of the founding fathers of Israel's cybersecurity eco-system heads the Blavatnik ICRC: Major Gen. (Ret.) Prof. Isaac Ben-Israel.

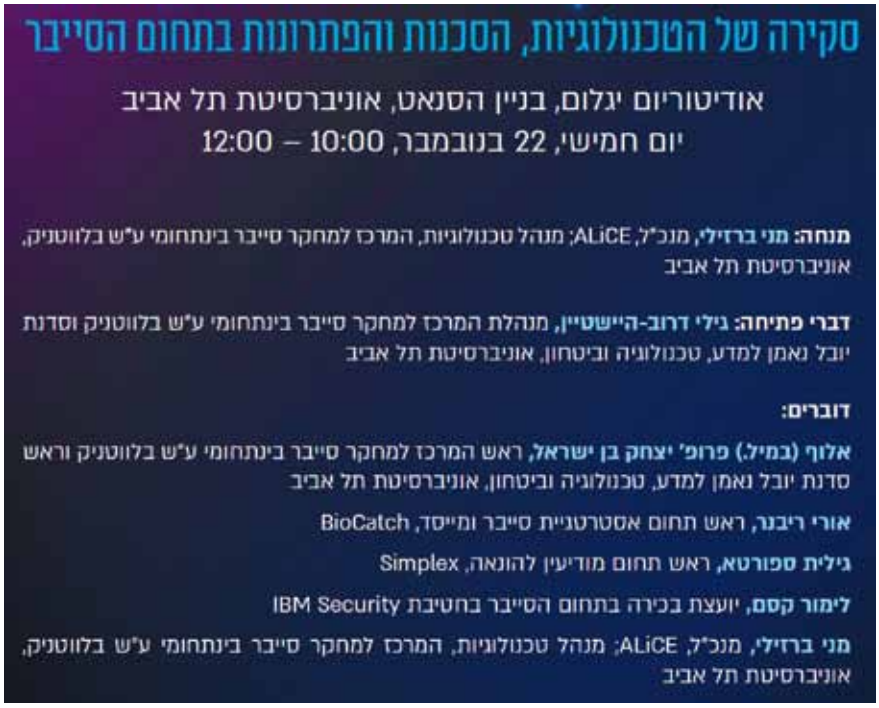
This tailor-made program frames the central aspects of cybersecurity on the national level, providing insights and applicable tools. The typical program consists of five full days of studies and activities: Academic lectures, class discussion and workshops, as well as field studies through visits to cybersecurity stakeholders. Some key takeaways from the program:

- Core elements in designing an effective cybersecurity strategy
- How to support a sustainable cyber ecosystem
- Unified understanding of technical and non-technical foundations of cybersecurity
- Capability to gauge full consequences of cybersecurity threats
- Capability to evaluate responses to cybersecurity threats and events See Appendix D for the full marketing brochure.

School Pupils: Tomorrow's Leaders

The human resource shortage is a global cybersecurity challenge, with schools being the fundamental part of the solution. Committed to educating Israel's future leaders in cybersecurity, Blavatnik ICRC has long-standing ties with the Gifted Children's Program and the National Cyber Education Center. These efforts will continue in 2019 and will include the Youth Conference during Cyber Week. These programs focus on high-school pupils.

In November 2018, we ran a pilot event for Grade 4 pupils. We hosted 200 children for a two-hour session, where experts catered to the kids' curiosity with light and inspiring talks related to cybersecurity.



The Annual Youth Conference

The Annual Youth Conference, a joint initiative of the Blavatnik ICRC at Tel Aviv University and the Cyber Education Center, showcased case studies and lectures to 600 talented Israeli youth, tomorrow's cyber leaders. The Youth Conference is part of the Blavatnik ICRC's commitment to educate the next generation in cybersecurity related.

APPENDICES

icrc@post.tau.ac.il | Tel: +972-3-640-6041
www.icrc.tau.ac.il