TEL AVIV UNIVERSITY
Pursuing the Unknown

ICRC
Blavatnik Interdisciplinary
Cyber Research Center

THE BLAVATNIK INTERDISCIPLINARY CYBER RESEARCH CENTER

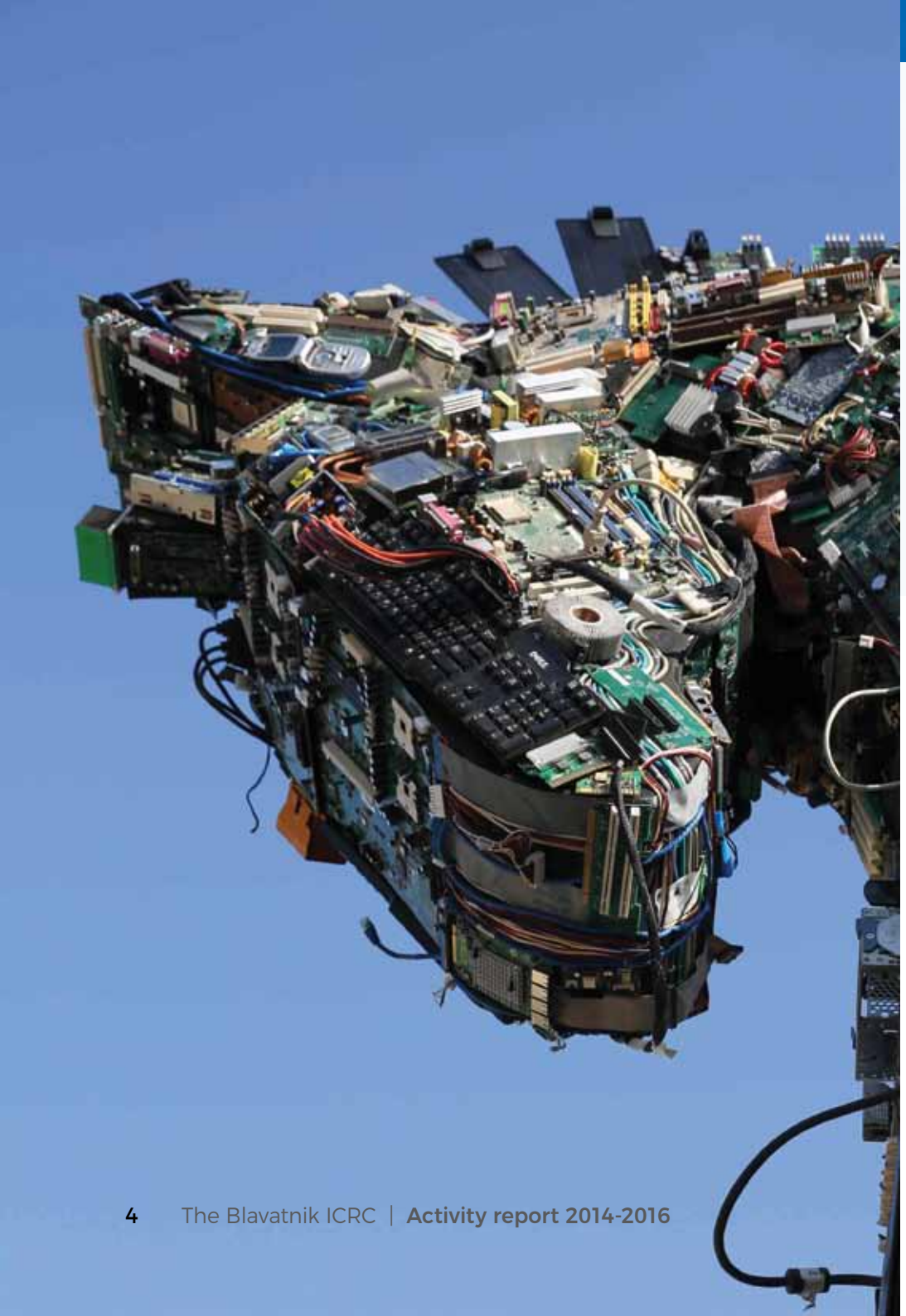
ACTIVITY REPORT 2014-2016

TEL AVIV UNIVERSITY (C), **2017**

Editors: Lior Tabansky, Dafna Kovler
Photography: Chen Galili
Design: Andrey Shir

Printed in Israel, 2017


2016
CYBERWEEK
ICR



CONTENTS

CONTENTS

THE BLAVATNIK INTERDISCIPLINARY CYBER RESEARCH CENTER

The Blavatnik Interdisciplinary Cyber Research Center (the ICRC) was established in 2014 at Tel Aviv University (TAU) as a joint initiative with the Israel National Cyber Bureau at the Prime Minister's Office, with the following goals:

- **Establish a leading global cyber research center.**
- **Boost the volume and quality of scientific research for cybersecurity.**
- **Attract researchers and advance academic training in cybersecurity.**
- **Become a center of knowledge on cyber.**

The ICRC is the first institutionalized Israeli government-academia cooperation in cyber-related research, inaugurated in September 2014 by Prime Minister Benjamin Netanyahu at TAU's 4th Annual Cybersecurity Conference. **Boasting 50 faculty members and more than 200 cyber researchers (predominantly research students and post-doctoral fellows) from different disciplines, the ICRC is the largest Cyber Research Center among Israel's universities.**

The Blavatnik ICRC epitomizes interdisciplinary research by nurturing profound cooperation across TAU's faculties, departments and schools including Exact Sciences, Computer Sciences, Law, Engineering, Social Sciences, Management and Humanities. The ICRC funding is devoted to competitive research grants carried out throughout Tel Aviv University (TAU), Israel's largest research and higher learning institution, boasting over 29,000 students studying in nine faculties and 125 schools and departments across the sciences, humanities and the arts. Almost half of the cohort are graduate students. Situated in Israel's economic and technological capital, TAU shares Tel Aviv's unshakable spirit of innovation and openness. The Blavatnik ICRC builds on TAU's researcher excellence and 12 years of the active cybersecurity policy-oriented university research hub: the Yuval Ne'eman Workshop for Science, Technology, and Security.

GOVERNANCE

The Blavatnik ICRC is governed by executive management, and scientific, steering and advisory committees.

EXECUTIVE MANAGEMENT

The chief executives of the Blavatnik ICRC are:

- Major Gen. (Ret.) Prof. Isaac Ben Israel, Head
- Prof. Avishai Wool, Deputy Director
- Prof. Ran Canetti, Chairman of the Scientific Committee
- Dr. Yaniv Harel, Head of Research Strategy
- Jacob Mendel, MBA, Head of Industry Research Cooperation
- Gili Drob-Hiesten, Executive Director

SCIENTIFIC COMMITTEE

The Scientific Committee has the following roles:

1. Propose missions, goals and annual and long-term indices in order to achieve the ICRC's goals, missions and research fund criteria.
2. Recommend areas of practice in the ICRC.
3. Recommend activities and events the ICRC should host.
4. Offer investments in infrastructure that the ICRC requires.
5. Examine research proposals in order to choose research that will be financed by the research fund and recommend the level of funding to be received.
6. Recommend world-renowned scholars in the field that should be invited to take part in the ICRC's activities.

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

- Prof. Ran Canetti, Chairman of the Scientific Committee
- Major Gen. (Ret.) Prof. Isaac Ben Israel, the Head of the Blavatnik ICRC
- Prof. Avishai Wool, the Deputy Director of the Blavatnik ICRC
- Prof. Mooly Sagiv
- Dr. Eran Toch
- Prof. Michael Birnhack
- Dr. Ohad Barzilay
- Prof. Tammie Ronen Rosenbaum
- Prof. Udi Sommer
- Prof. Leo Corry
- Prof. Inna Weiner

THE BLAVATNIK INTERDISCIPLINARY CYBER RESEARCH CENTER

STEERING COMMITTEE

The Steering Committee, composed of TAU and Israel National Cyber Bureau representatives, has the following roles:

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

ADVISORY BOARD

- Prof. Joseph Klafter, President, TAU
- Prof. Jacob A. Frenkel, Chairman of the Board of Governors, TAU
- Dr. Giora Yaron, Chairman of the Executive Council, TAU
- Brig. Gen. (Res.) Nadav Zafrir, Former commander Israel Defense Forces Unit 8200
- Brig. Gen. (Res.) Dr. Danny Gold, Head of Administration for the Development of Weapons and Technological Infrastructure (MAFAT), Ministry of Defense and the Head of the Israel National Committee for Commercial-Civilian Cyber R&D
- Dr. Shlomo Markel is Chairman of the Board of Directors of RAMOT (TAU's technology transfer company) and Vice President of Broadcom Corporation

RESEARCH

The Blavatnik ICRC epitomizes interdisciplinary research, enabling and supporting profound cooperation across TAU's faculties, departments and schools including Exact Sciences, Computer Sciences, Law, Engineering, Social Sciences, Management and Humanities.

The Blavatnik ICRC has solicited research proposals from teams led by TAU Principal Investigator in two competitive rounds: The first Call for Research Proposals (CFP) was published in November 2014, for the 2014 and 2015 budget years; the second Call for Research Proposals published in May 2016.

The ICRC solicited research proposals from teams led by TAU Principal Investigator in several tracks:

1. Exploratory research. The cap is NIS 80,000 and the duration of the research project is up to one year.
2. Single Principal Investigator (PI). These proposals are capped at NIS 250,000 per year.
3. Collaborative proposals with two or more PIs, either from the same academic unit or from different units. The cap is NIS 600,000 per year.
4. Interdisciplinary proposals of three or more PIs from different academic disciplines. The cap is NIS 1,000,000 per year.
5. Co-funded by one or more companies and the ICRC, was added. Proposed projects can last up to 3 years with up to NIS 1,200,000 per year. The expectation is of roughly even split in funding between the ICRC and the companies involved.

ELIGIBILITY

A Principal Investigator can be any prominent professional in the relevant topic of research. In academic & industry proposals, the lead PI must be senior academic staff member at TAU. In exploratory proposals, the PI has to be either a member of the senior academic staff of TAU, be a PhD student or a post-doctoral researcher at TAU. In the latter two cases, a support letter from a member of the senior academic staff at TAU must be provided.

The research proposals were evaluated in a multi-stage peer-review process by the scientific committee and external referees, according strictly to academic criteria: scientific excellence, novelty, applicability to cyber security, and inter-disciplinarity. The Blavatnik ICRC has awarded grants to 56 winning teams in total, selected from 101 proposals, submitted by TAU faculty member-led teams between November 2014 and May 2016.

The Blavatnik ICRC has awarded grants to 56 winning teams, selected from 101 proposals between 2014-2016

GRANTS AWARDED, 2014-2016, LISTED IN ALPHABETICAL ORDER

Researchers	Research Title
David Horn	Adapting Quantum Clustering (QC) and Related Algorithms to Anomaly Detection in Big Data
Yuval Shavitt	Advanced Attacks against Internet Security Protocols
Amir Averbuch	Anomaly Detection for Critical Infrastructure Protection: Second Generation
Amnon Ta-Shma; Alon Rosen	Anonymous and Secure Electronic Voting: Protecting our Democratic Infrastructure
Hanoch Levy; Eli Brosh (Canary Connect); Gil Zussman (Columbia University)	Attack Resilient Resource Placement in Cloud Computing System and Power Grid
Avishai Wool; Gabi Shugul (Astronautics C. A. Ltd); Raz Tikochinski (Astronautics C. A. Ltd)	Avionic bus cyber attack identification
Deborah Housen-Couriel	Balancing National Security and Privacy Rights to Privacy and the Rule of Law in Democratic Societies a Comparative Analysis
Noam Rinetzky; Sharon Shoham	Best Practices for Verifiably-Correct Concurrent Systems
Yossi Azar	Co-Location-Resistant Clouds Security
Deganit Paikowsky; Gil Baram	Confess or Deny? Strategies for Dealing with Cyber Attacks
Lior Wolf	Compilation Integrity Assurance through Deep Code Alignment
Roey Tzezana	Crime and IoT
Udi Sommer; Gahl Silverman (Bar-Ilan University)	Cyber Jihad Taxonomy: Qualitative Analysis of the Behavior of Jihadi Members on Social Networks
Aviram Zrahia	Cyber Information Sharing in a Competitive and Conflicted Environment

Researchers	Research Title
Amir Lupovici; Deganit Paikowsky; Or Rabinowitz (HUJI); Dimitry (Dima) Adamsky (IDC)	Cyber, Space and Nuclear Weapons Analogies, Interrelations and Differences in forming National Strategy – A Comparative Analysis of the United States and Russia (USSR)
Tal Soffer	Cyber Security Technology Foresight
Ohad Barzilay; Gal Oestreicher-Singer; Hilah Geva	Cyber Threats in Self-Regulating Digital Platforms
Lior Tabansky	Cybersecurity Theory Development: the Israeli Case in Strategic Context
Amir Globerson; Matan Gavish (HUJI); Ronen Talmon (Technion)	Detection of Cyber Attacks in Industrial Control Systems by Intrinsic Sensor Data Analysis
Gil Baram	The Deniability Mechanism in the Cyber Age – Its Effect on States' Behavior in the International System
Eli Amir; Shai Levi	Do Firms Under-Report Information on Cyber Attacks? Evidence from Capital Markets
Naama Tzur; Lior Zalmanson; Gal Oestreicher-Singer	The Effect of Engagement on Private Information
Tomer Geva; Maytal Saar-Tsechansky (U. Texas Austin)	Economic Utilization of Workforce-Based Labeling for Security Applications
Joachim Meyer; Ronen Avraham	Evolving Cyber-Threats and Countermeasures: Mathematical, Behavioral and Legal Perspectives
Yehuda Afek; Anat Bremler-Barr; Edith Cohen (IDC)	Extracting Signatures and Filters for Zero-day Sophisticated DNS and other DDoS Attacks
Eran Toch	Guiding and Incentivizing Cyber-Security Behavior
Tova Milo; Daniel Deutch	Infrastructure for Cyber Threat Information Sharing
Lior Tabansky; Margarita Jaitner (Swedish Defence College)	Hostile Influence Operations via Social Media: A Cybersecurity Issue? Assessing the Applicability of Recent Evidence to the Israeli Soft Power
Irad Ben-Gal; Doron Cohen	Identification of Malicious Websites by Learning the Websites' Design Attributes

Researchers	Research Title
Shachar Reichman; Sam Ransbotham (Boston college); George Westerman (MIT)	The Interplay of Cyber Vulnerability and Enterprise Credit Risk
Deborah Housen-Couriel	The Intersection of Cybersecurity and Space Security: New Threats and the Development of Legal and Policy Responses
Oded Maimon; Shuyuan Mary Ho (Florida State University)	A Machine Learning Collaborative Study of Language-Action Cues for Spontaneous Deceptive Communication and Cyber-Ontology Development
Avishai Wool; Leonid Lev (Israel Electric Company)	Network Attack and Detection in Modbus/TCP SCADA Systems
Ohad Barzilay; Asher Tishler (College of Management); Amitai Gilad	Mitigating the Risk of Advanced Cyber-Attackers
Roy Zuckerman	Non-Public Financial Information Leak
Ina Weiner	Novel Method for Insider Threat Detection
Benny Chor; Metsada Pasmanik-Chor	Personal Genomic Data: Privacy and Security Aspects
Avishai Wool	Photonic Emission Side-Channel Cryptanalysis of Secure Hardware Devices
Michael Birnhack; Avner Levin (Ryerson, Canada)	Privacy by Design by Legislation
Nahum Kiryati	Reconciling Cyber-Security Research with Privacy Law: The Video Analytics and Medical Image Analysis Examples
Amos Fiat; Iftach Haitner; Eran Tromer; Benny Applebaum	Robust Decentralized Digital Currency

Researchers	Research Title
Shahar Maoz; Eran Toch; Eran Tromer	Safety and Privacy of Mobile Applications through Model Inference
Noam Rinetzky; Mooly Sagiv	Scaling Symbolic Reasoning for Executable Code via Summarization and Interaction
Sivan A. Toledo; Eran Tromer; Shay Gueron (Haifa University)	Securing Servers and Endpoints using Software Guard Extensions
Ayala Arad; Stefan Penczynski (University of Mannheim)	Strategic Cyber Reasoning in Attacker-Defender Resource Allocation Games
Neil Gandal; Tyler Moore (SMU)	Shocks to and Security in the Bitcoin Ecosystem: An Interdisciplinary Approach
Michael Birnhack; Tali Hatuka; Issachar Rosen-Zvi; Eran Toch	Smart Cities Cyber Security (SCCS)
Yael Steinhart; Jacob Goldenberg	The Selfish and Caring of Sharing: Exploring the Reasons and Personal Outcomes of Public-Shaming
Lior Tabansky	Towards a Theory of Cyber Power: Security Studies, Meta-governance, National Innovation System
Yuval Shavitt	Understanding IP Hijack Events
Jacob Scheuer	Ultralong Fiber Laser for Secure Communications
Amir Lupovici	Violence and the (Social) Construction of Cyber Deterrence
Gal Sheppes; Roy Luria	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
Keren Elazari	What's the Value of Bug Bounty Programs?

See Research Abstracts from page 38 below

THE BLAVATNIK INTERDISCIPLINARY CYBER RESEARCH CENTER

CAPACITY BUILDING

The ICRC develops capability to enable cutting-edge research.
The ICRC provides workspace for 25 researchers as well as a conference room.
The ICRC has procured a complex technical infrastructure for research in 2015, including Big Data Analytics solution from Oracle.
The ICRC has procured a custom designed lab of GPU workstations to assist in Deep Learning research.
The ICRC allocates dedicated grants to support undergraduate and graduate students as well postdoctoral fellows who conduct research in relevant topics.
The ICRC supports workshops, seminars and other activities in relevant topics, held throughout the university.

RESEARCH SEMINARS

Date	Title	Speakers
26.07.16	Crime, Terror and the Internet of Things	**Dr. Roey Tzezana**, ICRC
07.06.16	How New Surveillance Technologies Enter Our Lives: The Case of School CCTV	**Prof. Michael Birnhack**, Faculty of Law
26.05.16	Strategic Defense	**Prof. Sandro Gayken**, director of the Digital Society Institute at the ESMT, Berlin
17.05.16	Network Security, Vulnerabilities and Disclosure Policy	**Prof. Neil Gandal,** School of Economics
10.05.16	A Three Layer Framework for a Comprehensive National Cyber Security Strategy	**Lior Yaffe**, Head of Defense Planning in the INCB and a PhD candidate in Tel Aviv University
15.03.16	Professional Perspectives of Cybersecurity	**Dr. Yaniv Harel**, EMC-Dell & ICRC
29.12.15	Behavioral aspects of cyber security	**Prof. Joachim Meyer**, Department of Industrial Engineering
29.12.15	Coping with Physical Attacks on Fiber Networks and Power Grids	**Mr. Omer Gold**
03.06.15	Time Sensitive Collaborations using Cryptographic Protocols	**Prof. Shafi Goldwasser,** MIT & Weizmann Institute
13.05.15	Controlling information channels across the software/ hardware boundary	**Prof. Andrew Myers**, Cornell University
09.02.15	ICRC Researchers Forum	
12.01.15	Privacy by Design	**Prof. Michael Birnhack**, Faculty of Law

INTERNATIONAL ACADEMIC COLLABORATIONS

Partner

With The University of Modena and Reggio Emilia (UniMoRE), Modena, Italy

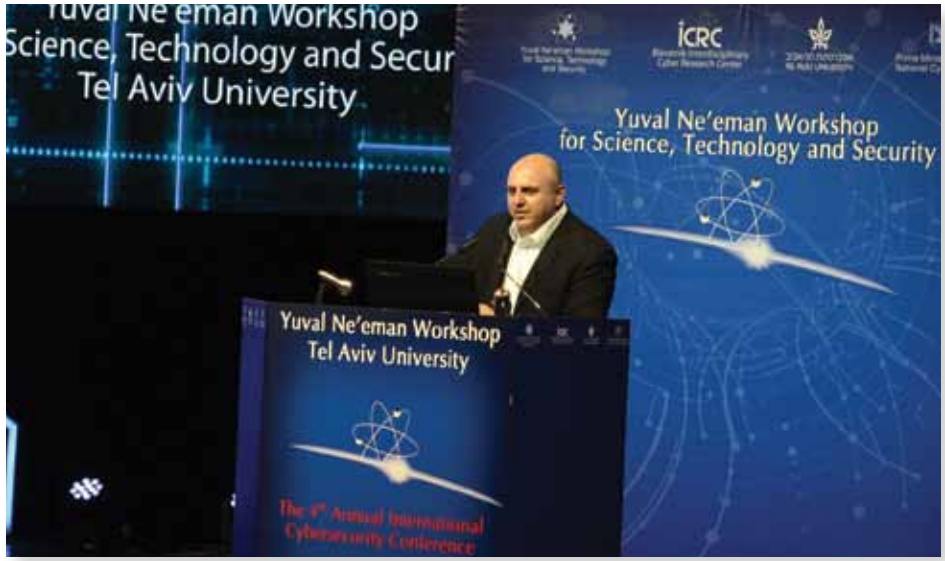
With Singapore National Research Foundation

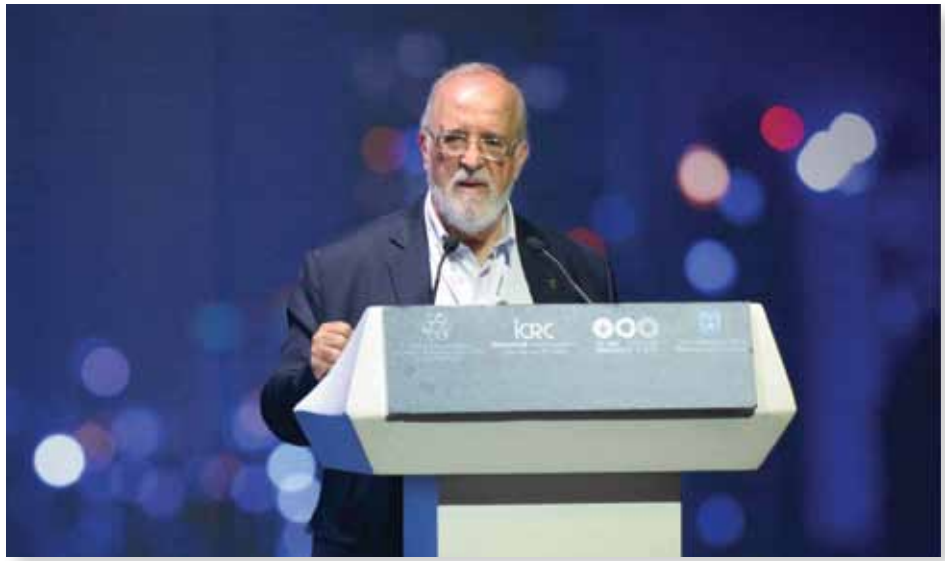
With The Indian Institute of Technology (IIT), Kanpur, India

With The European School of Management and Technology (ESMT), Berlin, Germany

WAR-GAMING (SIMULATION)

The ICRC performs unique complex simulations together with SIMLAB. The three latest war-games simulated real-time cybered disruptions to a diverse group of participants, thus exploring effects on strategic and operational decision making processes in realistic conditions of uncertainty.





OUTREACH

The Blavatnik Interdisciplinary Cyber Research Center develops scientific approaches to address future as well as current issues, thus creating direct policy relevance. Outreach activity is an integral part of ICRC and is crucial for the mission. The ICRC established several independent outreach formats, each vendor-neutral as well as free of cost for all participants.

SENIOR CYBER FORUM

The ICRC hosts the Senior Cyber Forum: invite-only strategic forum for experts, visionaries and decision makers, which was established by The Yuval Ne'eman Workshop in TAU in 2011. The Senior Cyber Forum periodically convenes several dozen independent activists, government representatives, top executives, TAU researchers, investors and dignitaries. It provides an informal professional, neutral, intimate environment that enables confidential discussions and builds trust. Designed to transcend existing barriers and promote cooperation between civil society, government agencies, academia, business, industry, venture capital funds, defense practitioners, law enforcement agencies and others, it attracts many senior experts.

THEMATIC CONFERENCES

The ICRC runs periodic Thematic Conferences, together with the Yuval Ne'eman Workshop in TAU. The typical audience for a half-day conference is 600 people, comprised of general public, various stakeholders, professionals and students.

AMBASSADORS' SUMMIT CONFERENCES

Israel and Tel Aviv University are continuously acknowledged as centers of innovation and scientific excellence. Israel has gained a leading cybersecurity reputation, and indeed offers insights into shared challenges and opportunities as well as offers assistance. Foreign diplomatic corps are an important target audience. On top of traditional duties, some nations already have a cyber attaché in Israel. The Blavatnik Interdisciplinary Cyber Research Center has established the Ambassadors' Summit conferences as a dedicated venue to facilitate discussion and spur cooperation with potential partners throughout likeminded nations.


ICRC
Blavatnik Interdisciplinary Cyber Research Center
אוניברסיטת תל אביב
The Blavatnik Interdisciplinary Cyber Research Center cordially invites you to attend the:
2ND
February 18th, 2016
AMBASSADORS SUMMIT
Thursday, February 18th, 2016, between 14:00-18:00
Location: The Green Villa, 24 George Wise St., Tel Aviv
14:00-14:30 REGISTRATION & REFRESHMENTS
14:30-15:15 OPENING REMARKS
Prof. Maj. Gen. (Ret.) Isaac Ben-Israel, Head of the Blavatnik Interdisciplinary Cyber Research Center (ICRC) and Head of the Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University
Mr. Iddo Moed, Cyber Security Coordinator, Ministry of Foreign Affairs
Ambassador Alon Roth-Snir, Ministry of Foreign Affairs
Dr. Giora Yaron, Chairman of the Executive Council, Tel Aviv University
15:15-16:00 LECTURES
Dr. Eviatar Matania, Head of the Israeli National Cyber Bureau, Prime Minister's Office
Prof. Joachim Meyer, Department of Industrial Engineering, Tel Aviv University
Brig. Gen. (Res.) Dr. Daniel Gold, CEO & Founder, Gold R&D Technology and Innovation Ltd., and Head of the Israel National Committee for Commercial/Civilian Cyber R&D
Dr. Udi Sommer, Political Science Department, Tel Aviv University
16:00-16:45 NETWORKING & REFRESHMENTS
16:45-18:00 LECTURES
Prof. Michael Birnhack, Buchman Faculty of Law, Tel Aviv University
Keren Elazari, Analyst and Cybersecurity Researcher, the Blavatnik Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University
Matan Scharf, Strategic Advisor to the Blavatnik Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University
Menny Barzilay, Strategic Advisor to the Blavatnik Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University


ICRC
Blavatnik Interdisciplinary Cyber Research Center
TEL AVIV UNIVERSITY אוניברסיטת תל אביב
Prime Minister's Office
National Cyber Directorate
In cooperation with:
Ministry of Foreign Affairs
Israel
3RD AMBASSADORS SUMMIT
Monday, February 6th, 2017
09:30– 14:00
New dimensions in cyber space:
Web on Fire - Incitement Online
Rebecca and Jacob Zeevi Auditorium, Beit Hatfutsot,
Tel Aviv University Campus
Beit Hatfutsot is located on the campus of Tel-Aviv University, Klausner Street, in Ramat Aviv.
Entrance through Matatia Gate 2.
The digital domain is a key facilitator for growth and prosperity.
How can terrorism and criminal abuse online be controlled and prevented?
09:30 – 10:00 Reception
10:00 – 11:15 Lectures
Major Gen. (Ret.) Prof. Isaac Ben-Israel, Cyber Week 2017 Chairman & Director, ICRC - Blavatnik Interdisciplinary Cyber Research Center
MK Ayelet Shaked, Minister of Justice
Dr. Eviatar Matania, Director General of the Israel National Cyber Directorate, Prime Minister's Office
Prof. Yaron Oz, Rector, Tel Aviv University
Liat Killner, Adv., Legal Counsel, National Cyber Crime Unit
Lior Tabansky, Researcher, Blavatnik Interdisciplinary Cyber Research Center & Doctoral Candidate at the School of Political Science, Government and International Affairs, Tel Aviv University
11:15– 11:45 Networking Break
11:45– 13:00 Lectures
Mili Bach, Former Head of Enforcement & Investigation Department, The Israeli Law, Technology and Information Authority, Ministry of Justice
Daniel Cohen, Researcher, Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University
Deborah Housen-Couriel, Researcher, Legal and Policy Expert on Cybersecurity and Regulation, Blavatnik ICRC & Yuval Ne'eman Workshop, Tel Aviv University
Ilan Graicer, Strategic Advisor, Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University
Dr. Marina Shorer, NSG College
13:00 – 14:00 Lunch

THE ANNUAL CYBER WEEK

Since 2011, the free-to-attend Tel Aviv University Annual International Cybersecurity Conference attracts thousands of visitors. Since 2014, the Blavatnik ICRC conducts the event which has grown to become the national Cyber Week, comprised of dozens of conferences, thematic workshops, and networking events. Target audiences encompass global academic researchers, policy makers, defense practitioners, diplomats, tech entrepreneurs, multinational business, Israeli start-ups, high-school students, independent hackers, civil activists, media and general public. The Main Plenary held at the 1,200 seat Smolarz Auditorium provides a unique opportunity to hear from global experts. Further, video presentations and conference proceedings are freely available on the Web. The campus becomes the host of several dozen workshops, seminars, round-tables and other less-formal events the Blavatnik ICRC organizes jointly with numerous global partners. School pupils and business executives; hackers and law enforcement professional; diplomats and academics; corporate investors and journalists; IDF soldiers and entrepreneurs; IT-pros and policy makers from all over the world - convene in Tel Aviv University at ICRC Cyber Week. June 2016, we were honored to host more than 5,000 attendees from over 50 countries, fortifying the Blavatnik ICRC as the host of the largest cyber conference outside the U.S.

CYBER INNOVATION: THE NEXT GENERATION

Sunday, September 14th 2014

09:00-19:00 | Smolarz Auditorium, Tel Aviv University

09:00-10:30 **Welcome Reception & Registration**

10:30-11:00 **Opening Session**

Conference Chairman: **Major Gen. (Ret.) Prof. Isaac Ben Israel**, Head of ICRC & Yuval Ne'eman Workshop, Tel Aviv University

Prof. Joseph Klafter, President of Tel Aviv University

Prof. Jacob A. Frenkel, Chairman of the Board of Governors, Tel Aviv University, Chairman of JPMorgan Chase International, Former Governor of Bank of Israel

Introduction to the Yuval Ne'eman Workshop for Science, Technology & Security

Gili Drob-Heistein, Executive Director

Dr. Roey Tzezana, Fellow & Researcher, Yuval Ne'eman Workshop for Science, Technology & Security, Tel Aviv University

11:00-11:40 **The Frontline of Cybersecurity**

Chairman: **Dr. Giora Yaron,** Chairman of the Executive Council, Tel Aviv University, Chairman of Ramot

Gen. (Ret.) Keith Alexander, CEO and President, Iron Net; Former Director, National Security Agency (NSA), U.S.

Nadav Zafrir, Co-Founder of Tearn 8-Cyber Security Venture Creation, Former Head of 8200 Unit (IDF)

11:40-12:00 **Today's Security for Tomorrow's Threats**

Amnon Bar-Lev, President, Check Point Software Technologies

CYBER WEEK 2014

13:00-14:15 **First Session: Cyber Innovation**

Chairwoman: Keren Elazari, Fellow, Yuval Ne'eman Workshop for Science, Technology & Security, Tel Aviv University

Avi Hasson, Chief Scientist, Ministry of Economy

Secretary Gordon R. England, Partner at Glilot Capital, Former Deputy Secretary of Defense, U.S.

Esti Peshin, Director, Cyber Programs, IAI

Lawrence Pingree, Research Director, Gartner

Mark Gazit, CEO, Theta Ray

14:15-15:15 **Second Session: Hacking the Brain**

Chairman: Yanki Margalit, Social Entrepreneur, Chairman, SpaceIL, Partner, Innodo Ventures

Prof. Nathan Intrator, Blavatnik School of Computer Science, Sagol School of Neuroscience, Tel Aviv University

Dr. Yossi Yovel, Dept. of Zoology, Life Sciences Faculty, Sagol School of Neuroscience, Tel Aviv University

Dr. Roey Tzezana, Fellow & Researcher, Yuval Ne'eman Workshop for Science, Technology & Security, Tel Aviv University

Dr. Moran Cerf, Professor of Neuroscience, Kellogg School of Management & NYU, and Ex-Security Expert

15:15-15:50 **Networking Break**

15:50-16:40 **Third Session: The Secrets Behind a Successful Start-Up Panel**

Moderator: Izhar Shay, Managing Partner, Canaan Partners Israel

Yoav Tzruya, Partner, JVP Cyber Labs

Dr. Orna Berry, Corporate VP, Growth and Innovation, EMC Centers of Excellence, EMEA and the U.S.

Yuval Shachar, Marker, LLC & Innovation Endeavors Partner

Amir Orad, Former CEO, NICE Actimize, Co-Founder, Cyota, BillGuard Board

16:40-18:00 **Fourth Session: Internet of Things**

Chairman: Nir Peleg, Head of R&D Division, Israeli National Cyber Bureau

Shmuel (Mooly) Eden, Senior VP, GM Perceptual Computing, President, Intel Israel

S. Ramadorai, Vice Chairman, Tata Consultancy Services Ltd; Chairman, the National Skill Development Agency (NSDA), India

Arik Mimran, Vice President, Qualcomm Israel Ltd.

Daniel Jammer, President and Founder, Nation-E

18:00-18:30 **Closing Session**

Major Gen. (Ret.) Uzi Dayan, Chairman, National Lottery Mifal Hapayis

Prof. Joseph Klafter, President of Tel Aviv University

Avi Fischer, Chairman and CEO of Clal Industries Ltd.

Dr. Eviatar Matania, Head of the Israeli National Cyber Bureau

18:30 **Prime Minister of Israel, Benjamin Netanyahu**

CYBER INNOVATION: THE FUTURE OF CYBERSECURITY

Monday, September 15th 2014

07:30-19:40 | Smolarz Auditorium, Tel Aviv University

07:00-08:30 **Welcome Reception & Registration**

10:30-11:00 **Opening Session**

Conference Chairman: **Major Gen. (Ret.) Prof. Isaac Ben Israel,** Head of ICRC & Yuval Ne'eman Workshop, Tel Aviv University

Opening remarks:
Minister of Defense, MK Moshe (Bogie) Ya'alon
The 9th President of Israel, Shimon Peres
Minister of Science, Technology & Space, MK Yaakov Perry

Shai Nitzan, Attorney General, Department of Justice, Israel
Steven Blaney, Minister of Public Safety and Emergency Preparedness, Canada
Sichung NOH, Chairman of KIBC and CEO of FEELUX

Introduction to the Yuval Ne'eman Workshop for Science, Technology & Security
Gili Drob - Heistein, Executive Director & **Ram Levi,** Senior Researcher, Yuval Ne''eman Workshop for Science, Technology and Security, Tel Aviv University

On War - the Influence of the Cyber Dimension
Dr. Haim Assa, Head of SIMLAB, the Lab for Policy & Security Simulations, Tel Aviv University

10:10-11:50 **First Session: New Approaches for Dealing with Emerging Threats**

Chairman: **Menny Barzilay,** Cybersecurity Strategist & Member of the Yuval Ne'eman Workshop Senior Cyber Forum

Eugene Kaspersky, Chairman and CEO, Kaspersky Lab

Lt. Col. (Ret.) William Hagestad, Author, Red Dragon Rising

Laurence Pitt, EMEA Director, Information Security Strategy, Symantec

Oded Ilan, Director of Sales, CyberGym

Major General (Ret.) Ido Nehushtan, Senior Strategic Adviser, EMC

Andrey Dulkin, Senior Director of Cyber Innovation, CyberArk

11:50-12:20 **Coffee Break**

12:20-13:20 **Second Session: National Cybersecurity Strategy & Challenges**

Chairman: **Michael Levinrad,** Head of International Cooperation Division, Israeli National Cyber Bureau

Christopher Painter, Coordinator for Cyber Issues, Office of the Secretary of State, U.S.

James Quinault, Director, Office of Cyber Security and Information Assurance (OCSIA), Cabinet Office, UK

Ambassador Sorin Ducaru, Assistant Secretary General of the Emerging Security Challenges Division, NATO

Iddo Moed, Cyber Security Coordinator, Ministry of Foreign Affairs, Israel

13:20-14:20 **Lunch Break**

CYBER WEEK 2014

4:20-15:30 **Third Session: The Next Generation of Cyber Technologies**

Chairwoman: Dr. Dorit Dor, VP Products, Check Point

Michael Fey, Executive VP, Chief Technology Officer and General Manager of Corporate Products, Intel Security Group

Sanjay Deshpande, Chief Executive Officer & Chief Innovation Officer, Uniken Inc.

Avivah Litan, VP Distinguished Analyst, Gartner

Josh Goldfarb, Chief Security Strategist, Enterprise Forensics Group, FireEye

Liran Tancman, CEO and Co-Founder, CyActive

15:30-16:40 **Fourth Session: National Cybersecurity - the Defense Industry Perspective**

Chairman: Rami Efrati, Former Head of the Civilian Sector Division, National Cyber Bureau; Advisory Board Member, Nation-E

Hudi Zack, Senior VP & Head of the Cyber Business Unit, Verint

Yochai Corem, VP Marketing & Products, Intelligence & Cyber Solutions, Elbit Systems

Haden A. Land, VP, Research and Technology, Lockheed Martin

Doron Rotem, Director, C4I and Cyber Defense, MLM Division, Systems Missiles & Space Group, IAI

16:40-17:10 **Coffee Break**

17:10-18:30 **Fifth Session: Threats to the Financial Sector**

Chairman: Gadi Tirosh, General Partner, JVP

Minister of Economy, MK Naftali Bennett

Michal Blumenstyk-Braverman, GM, Azure Cybersecurity, Microsoft

Zvika Naggan, Former Deputy CEO and CIO, Bank Hapoalim

Sunil James, Vice President, Bessemer Venture Partners

Idan Plotnik, CEO, Aorato

18:30-19:30 **Sixth Session: The Mobile Security Ecosystem - Threats & Opportunities Panel**

Moderator: Arik Mimran, Vice President, Qualcomm Israel Ltd.

Asaf Ashkenazi, Director of Product Management, Qualcomm

Gal Salomon, Chairman & Founder, Discretix

Wolfgang Hisserich, Vice President, Business Development and Global Alliances, Deutsche Telekom

Oded Zehavi, COO, Kaymera Technologies

19:30-19:40 **Closing Remarks:**

MG. Uzi Moscovitch, Head of IDF C4I / J6 Directorate

ACADEMIC PERSPECTIVES ON CYBERSECURITY CHALLENGES

Monday, September 15th 2014

10:30-13:00 | Kes Hamishpat Hall, Trubowicz Building, Tel Aviv University

10:00-10:30 **Reception & Registration**

10:30-11:40 Moderator: Dr. Yaniv Harel, Fellow, Blavatnik Interdisciplinary Cyber Research Center, TAU

The Global Cyber-Vulnerability Report
Prof. V.S Subrahmanian, Professor of Computer Science, University of Maryland and Head of the Center for Digital International Government

Implementations of Machine Learning Tools for Detecting Cyber Anomalies
Prof. Irad E. Ben-Gal, Head of the Department of Industrial Engineering & Management, TAU

Rebuilding Trust in Computing Platforms
Dr. Eran Tromer, Senior Lecturer , Blavatnik School of Computer Science, TAU

Cyber Threat: Achilles Heel of Space Systems?
Dr. Deganit Paikowsky, Senior Researcher, Yuval Ne'eman Workshop for Science, Technology and Security, TAU

11:40-12:00 **Coffee Break**

12:00-13:00 **Air-Gap and Cyber Security**
Prof. Yuval Elovici, Director, Deutche Telekom Laboratories, Ben-Gurion University of the Negev, Israel

Cyber Studies in International Relations: Future Directions and Priorities
Dr. Lucas Kello, Research Fellow, Belfer Center for Science and International Affairs, Harvard University

Discovering Weaknesses in Virtual Systems
Prof. Assaf Schuster, Head of the Technion Center for Computer Engineering & a Professor in the Computer Science Department, Technion, Israel Institute of Technology

Cybersecurity Through a Military Revolution Prism
Lior Tabansky, Senior Researcher, Yuval Ne'eman Workshop for Science, Technology and Security, TAU

HACK TALKS. THE TECHNOLOGICAL ASPECTS OF CYBERSECURITY

Monday, September 15th 2014

14:15-16:35 | Kes Hamishpat Hall, Trubowicz Building, Tel Aviv University

14:15-15:15 Chairman: **Guy Mizrahi,** CEO Cyberia (IAI Cyber Accessibility Center)

I Hunt TR-069 Admins: Abusing Your ISP's Superpowers
Shahar Tal, Malware & Vulnerability Research, Check Point

Did You Pack it Yourself: Injecting Backdoors Through Software Delivery
Irene Abezgauz, VP Product Management, Quotium

Mobile Authentication - Challenges and Future Directions
Asaf Ashkenazi, Director of Product Management, Qualcomm

Operation Blog Bot.
Itzik Vager, VP Product & Bus. Dev, Verint

15:15-15:35 **Break**

14:35-16:35 **Attacking the Linux PRNG on Android: Weaknesses in Seeding of Entropic Pools and Low Boot-Time Entropy**
David Kaplan, Senior Security Researcher, IBM Security Systems

How to Empty an ATM in 15 min.
Roi Cohen, Pre Sale Engineer, Cybertinel

Castling the Attacker: Cyber Counter Intelligence & Deception
Gadi Evron, Chairman of the Board, Israeli CERT Foundation

Mapping The Global Mobile Security Threat Landscape
Ariel Sakin, Skycure

CYBER WEEK 2014

CYBER REVOLUTION

Tuesday, June 23nd 2015

08:00-16:30 | Smolarz Auditorium, Tel Aviv University

08:00-09:00 **Welcome Reception & Registration**

09:00-10:00 **Conference Opening**

Conference Chairman: **Major Gen. (Ret.) Prof. Isaac Ben Israel,** Head of the Blavatnik Interdisciplinary Cyber Research Center and Head of Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University

Gili Drob-Heistein, Executive Director, ICRC - The Blavatnik Interdisciplinary Cyber Research Center, and Executive Director, Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University

Prof. Joseph Klafter, President of Tel Aviv University

Ambassador Daniel B. Shapiro, Ambassador of USA in Israel

Dr. Eviatar Matania, Head of the Israeli National Cyber Bureau (INCB), Prime Minister's Office, Israel

10:00-11:00 **Prime Minister Benjamin Netanyahu**

10:30-11:30 **First Session: The Secret of Cyber Success**

Brig. Gen. (Res.) Nadav Zafrir, Former Head 8200, CEO and Co-founder, Team8

Dean Brenner, Senior Vice President, Government Affairs, Qualcomm

Amnon Bar Lev, President, Check Point

Bob Kalka, Vice President, Security Business Unit, IBM

11:30-12:45 **Second Session: National Policy and International Cooperation**

Chairman: **Michael Levinrad,** Head of International Cooperation Division, Israeli National Cyber Bureau (INCB)

BG (NS) David Koh, Chief Executive, Cyber Security Agency, Singapore and Deputy Secretary (Technology) in the Ministry of Defence

The Honorable Howard A. Schmidt, Former Cyber Advisor to Presidents Barack Obama and George W. Bush; former CSO at Microsoft; former CISO at eBay

Dr. Kyung - Ho Chung, Vice President, Korea Internet & Security Agency

Rajendra S Pawar, Chairman & Co-Founder, NIIT Group & Founder, NIIT University, India

12:45-13:45 **Lunch Break**

13:45-15:00 **Third Session: Beyond Internet**

Chairwoman: **Dr. Orna Berry,** Corporate Vice President Growth and Innovation EMC Centers of Excellence EMEA and the US

Patrick M. Dewar, Executive Vice President, Lockheed Martin International

Brent Conran, Chief Information Security Officer, Intel

Asaf Ashkenazi, Director of Product Management, Qualcomm Technologies, Inc. (QTI)

Opher Doron, General Manager, MBT Space Division, Israel Aerospace Industries, Ltd. (IAI)

15:00-15:40 **Fourth Session:**

Chairwoman: **Michal Braverman-Blumenstyk,** General Manager, Azure Cybersecurity, Microsoft

Chen Bitan, General Manager, EMEA & APAC, CyberArk

Mark Gazit, CEO, ThetaRay

Maria Lewis Kussmaul, Co-Founder of AGC

15:40-16:30 **Fifth Session: Cybersecurity and Privacy - Views from Government, Industry and Academia**

Chairman: **Omer Tene,** Vice President of Research and Education, International Association of Privacy Professionals

Maureen K. Ohlhausen, Commissioner of the Federal Trade Commission, USA

Amit Ashkenazi, Legal Advisor, Israeli National Cyber Bureau (INCB)

Prof. Michael Birnhack, Professor of Law, Faculty of Law, Tel Aviv University

CYBER WEEK 2015

THE ACADEMIC PERSPECTIVE ON CYBERSECURITY CHALLENGES

Tuesday, June 23rd 2015

11:00-16:00 | Jaglom Auditorium, Tel Aviv University

11:00 **Opening: Dr. Yaniv Harel, Academic Conference** Co-Chair, Head of Research Strategy, ICRC, Tel Aviv University

1st Session: High Level Perspective

Global Malware Spread: Forecasting Infection Rates in 40 Countries

Prof. V.S Subrahmanian, Professor of Computer Science, University of Maryland and Head of the Center for Digital International Government

Internet security: Past, Present and Future - Fraunhofer SIT perspective

Prof. Michael Waidner, Director of Fraunhofer SIT, CASED and EC SPRIDE and Professor at TU Darmstadt

2nd Session: Economy & Policy

Political and Economic Coercion and a Post-Western Cybered World

Dr. Chris C. Demchak, RADM Grace M. Hopper Professor of Cyber Security and Co-Director, Center for Cyber Conflict Studies (C3S), Strategic Research Department, U.S.

Why does Research on Cybersecurity Need Economists?

Prof. Neil Gandal, Professor of Economics and Head of the Berglas School of Economics, Tel Aviv University.

Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad

Prof. Sharon Goldberg, Associate Professor, Computer Science, Boston University.

13:20 **Break & Lunch**

14:00 **3rd Session: Secure Computing & Networking**

Defending Against Internet Address Hijack

Prof. Yuval Shavitt, School of Electrical Engineering, Tel Aviv University

Private Set Intersection

Prof. Benny Pinkas, Professor in the Department of Computer Science, Bar- Ilan University

Techniques and Developments in Fast Garbling of Boolean Circuits

Prof. Yehuda Lindell, Professor at the Faculty of Computer Science Department, Bar-Ilan University

4th Session: Human Factors in Cyber

Risks Implications of Information Flow in Human Networks

Prof. Irad Ben Gal, Academic Conference Co-Chair, Chair of Department of Industrial Engineering, Tel Aviv University

Prof. Nathan Intrator, Blavatnik School of Computer Science, Sagol School of Neuroscience ,Tel Aviv University

How to Win at Cyber Security by Influencing People

Dr. Eran Toch, Senior Lecturer at the Department of Industrial Engineering, Tel Aviv University

15:40 **Research Presentation:**

Automated Risk Scoring of Web Users Based on Feedback Loop Browsing Model

Nancy Yacovzada & Michal Ben-Neria

Panel: Academic Cooperation

Dr. Tal Steinherz, Chief Technological Officer, Israel National Cyber Bureau

Triple Helix Research Networks for Strategic Priorities: An NTU Case Study.

Prof. Lam Khin Yong, Chief of Staff and Vice President (Research), Nanyang Technological University

Prof. Michael Waidner, Director of Fraunhofer SIT, CASED and EC SPRIDE and Professor at TU Darmstadt

CYBER WEEK 2015

CYBER REVOLUTION

Wednesday, June 24th 2015

08:00-15:30 | Smolarz Auditorium, Tel Aviv University

08:00-08:30 **Welcome Reception & Registration**

08:30-09:00 **Conference Opening**

Conference Chairman: **Prof. Maj. Gen. (Ret.) Isaac Ben Israel,** Head of the Blavatnik Interdisciplinary Cyber Research Center and Head of Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University

Gili Drob-Heistein, Executive Director, ICRC - The Blavatnik Interdisciplinary Cyber Research Center, and Executive Director, Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University

Dr. Giora Yaron, Chairman of the Executive Council, Tel Aviv University

Dr. Haim Assa, Head of SIMLAB, the Lab for Policy & Security Simulations, Tel Aviv University

09:00-09:30 **Sixth Session: Reinventing Cyber Security**

Chairman: **Matan Scharf,** Cyber Security Specialist, Researcher, and Entrepreneur

Gil Shwed, Founder, Chairman and Chief Executive Officer Check Point Software Technologies

Avi Hasson, Chief Scientist, Ministry of Economy

David Keren-Ya'ar, Science Oriented Youth

Shir Veltsman, Science Oriented Youth

09:30-10:00 **Moshe (Bogie) Ya'alon, Minister of Defense, Israel**

10:00-11:15 **Seventh Session: Rethinking Innovation**

Chairwoman: **Esti Peshin, Director,** Cyber Programs, Israeli Aerospace Industries

Matt Thomlinson, Vice President, Microsoft Cloud & Enterprise Security

Hudi Zack, Senior VP and Head of Cyber Business Unit, Verint

Dr. Dorit Dor, VP Products, Check Point

Dr. Yaniv Harel, General Manager of the Cyber Solutions Group of EMC

11:15-11:45 **Coffee Break**

11:45-12:00 **Introduction to the Yuval Ne'eman Workshop for Science, Technology & Security & The Blavatnik Interdisciplinary Cyber Research Center**

Menny Barzilay, Cybersecurity Strategist & Member of the Yuval Ne'eman Workshop Senior Cyber Forum

12:00-13:00 **Eighth Session: Cyber Security - Trend Setters**

Chairwoman: **Keren Elazari,** Fellow, Yuval Ne'eman Workshop for Science, Technology & Security, Tel Aviv University

Marion Marschalek, Reverse Engineering Maverick, Cyphort

Nicholas J. Percoco, Vice President of Strategic Services, Rapid7

Avivah Litan, Vice President Distinguished Analyst, Gartner

13:00-14:00 **Ninth Session: Sony: Lessons Learned**

Chairman: Zvika Naggan, Senior Advisor to Team8 and former CIO and Deputy CEO of Bank Hapoalim
Bruce Schneier, Internationally Renowned Security Technologist, The "Security Guru" according to the Economist
Rich Baich, Chief Information Security Officer (CISO) & Executive Vice President, Wells Fargo
Brig. Gen. (Res.) Nadav Zafrir, Former Head 8200, CEO and Co-founder, Team8

14:00-14:30 **Tenth Session: Brain & Machine Learning**

Chairman: Prof. Nathan Intrator, Blavatnik School of Computer Science , Sagol School of Neuroscience ,Tel Aviv University
Prof. Lior Wolf, Faculty Member at the School of Computer Science, Tel Aviv University
Dr. Oded Margalit, CTO of IBM CCoE

Parallel Track

Best Practices for Cyber Protection in Organizations

08:30-10:30
Jaglom Auditorium, Tel Aviv University

Parallel Track: Best Practices for Cyber Protection in Organizations. The INCB in collaboration with the ICRC invite you, CISO of companies and organizations, to take part in the launch of the Best Practices developed in order to increase cyber security

Parallel Track

Cyber Revolution in Military Affairs

11:00-13:00
Jaglom Auditorium, Tel Aviv University

A parallel track that will revolve around the topic of cyber security and how it affects and modifies the military world: defense doctrines, arms, deterrence, vulnerability, norms etc.
During the session we will hear from Israel's leading defense leaders.

Carmi Gillon, CEO of Cytegic and Former Head of the Shabak
Brig. Gen. (Ret.) Pinchas Barel Buchris, Partner, State of Mind Ventures
Brig. Gen. (Res.) Dr. Daniel Gold, CEO and Founder of Gold R&D Technology and .Innovation Ltd Head of the & Israel National Committee for /Commercial Civilian Cyber R&D
Brig. Gen. (Res.) Yair Cohen, Intelligence and Cyber Elbit Systems
Rear Admiral Ophir Shoham, Director of Defense Research and Development

CYBER WEEK 2015

THE ACADEMIC PERSPECTIVE ON CYBERSECURITY CHALLENGES

Sunday, June 19th 2016

09:00 – 17:30 | Beit Hatfutsot, Tel Aviv University

10:00 - 10:30 OPENING REMARKS:

Dr. Yaniv Harel, Conference Chairman and Strategic Advisor to the Blavatnik ICRC, Tel Aviv University

Prof. Yaron Oz, Rector, Tel Aviv University

Dr. Tal Steinherz, Chief Technological Officer, Israel National Cyber Bureau

10:30 - 11:45 1st SESSION: PRIVACY & LAW

Chair: **Prof. Michael Birnhack**, Professor of Law, Faculty of Law, Tel Aviv University

Prof. Susan Landau, Professor of Cybersecurity Policy, Department of Social Science and Policy Studies, Worcester Polytechnic Institute

Prof. Susan Freiwald, Professor of Law, Dean's Circle Scholar, University of San Francisco

Prof. David Thaw, Assistant Professor of Law and Information Sciences, University of Pittsburgh and Affiliated Fellow, Information Society Project, Yale Law School

11:45 - 12:45 2nd SESSION: ENCRYPTION & DECRYPTION

Chair: **Dr. Yaniv Harel,** Conference Chairman and Strategic Advisor to the Blavatnik ICRC, Tel Aviv University

Prof. Engin Kirda, Professor of Computer Science and Engineering, Northeastern University and Director of Northeastern Information Assurance Institute-Boston

Dr. Eran Tromer, Associate Professor, Department of Computer Science, Tel Aviv University

Prof. Avishai Wool, Deputy Director, Blavatnik ICRC, Tel Aviv University

12:45 - 13:30 LUNCH & NETWORKING

13:30 - 15:00 3rd SESSION: BEHAVIORAL ASPECTS OF CYBERSECURITY

Chair: **Prof. Joachim Meyer,** Professor, Department of Industrial Engineering, Tel Aviv University
Dr. Eran Toch, Senior Lecturer, Department of Industrial Engineering, Tel Aviv University
Prof. Sheizaf Rafaeli, Founding Director of the Center for Internet Research, University of Haifa
Dr. Chris Demchak, RADM Grace M. Hopper Professor of Cyber Security and Co-Director, Center for Cyber Conflict Studies (C3S), U.S. Naval War College

15:00 - 16:30 4th SESSION: CYBERSECURITY TECHNOLOGIES

Chair: **Dr. Yaniv Harel,** Conference Chairman and Strategic Advisor to the Blavatnik ICRC, Tel Aviv University

Prof. V.S Subrahmanian, Professor of Computer Science, University of Maryland and Head of the Center for Digital International Government

Prof. Dan Boneh, Professor of Computer Science, Head of the Applied Cryptography Group and Co-Directs of the Computer Security Lab, Stanford University

Prof. Yuval Shavitt, School of Electrical Engineering, Tel Aviv University

Prof. Thambipillai Srikanthan, Head of the Computer Science Department and Executive Director of the Cybersecurity Research Center, Nanyang Technological Univesity (NTU)

Prof. Yuval Elovichi, Faculty of Engineering Sciences, Ben Gurion University of the Negev

16:30 - 17:30 POSTERS EXHIBITION

CYBER WEEK 2016

THE 6TH ANNUAL INTERNATIONAL CYBERSECURITY CONFERENCE

Monday, June 20th 2016

08:00-16:00 | Smolarz Auditorium, Tel Aviv University

09:00 - 11:00 GREETINGS & OPENING REMARKS:

Conference Moderator: **Menny Barzilay,** Strategic Advisor, Blavatnik ICRC; CEO, FortyTwo

Conference Chairman: **Major Gen. (Ret.) Prof. Isaac Ben-Israel,** Head of the Blavatnik Interdisciplinary Cyber Research Center (ICRC); Chairman, Yuval Ne'eman Workshop for Science, Technology & Security, Tel Aviv University

Gili Drob-Heistein, Manager, Blavatnik Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University

Prof. Joseph Klafter, President, Tel Aviv University

Dr. Eviatar Matania, Head of the Israel National Cyber Directorate, Prime Minister's Office

Prime Minister Benjamin Netanyahu

Alejandro N. Mayorkas, Deputy Secretary, Homeland Security, USA

MK Ayelet Shaked, Minister of Justice, Prime Minister's Office

Zhao Zeliang, Director General, Bureau of Cyber Security, CAC.

11:00 - 12:15 1ST SESSION: CYBER FAST FORWARD

Chair: **Michal Braverman-Blumenstyk**, General Manager, Azure Cybersecurity, Microsoft

Omar Abbosh, Chief Strategy Officer, Accenture

Gil Shwed, Founder and CEO, Check Point Software Technologies

Caleb Barlow, Vice President, IBM Security

Udi Mokady, Founder, President and CEO, CyberArk

12:15 - 13:15 2ND SESSION: SPOTLIGHT ON CYBER INNOVATION

Chair: **Dr. Dorit Dor,** Vice President of Products, Check Point Software Technologies

Bharat Shah, Corporate Vice President, Microsoft Azure

Nadav Zafrir, Co-Founder, CEO, Team8

Dr. Douglas Maughan, CSD Director, Homeland Security Advanced Research Projects Agency, USA

13:15 - 14:00 LUNCH & NETWORKING

14:00 - 15:00 3RD SESSION: BUILDING CYBER, PROTECTING INFRASTRUCTURE (PANEL)

Moderator: **Kim Zetter,** Investigative Journalist & Author, Wired

Mark Gazit, CEO, ThetaRay

Richard Puckett, Senior Director, Security Operations & Cyber Intelligence, General Electric

Terry Roberts, Founder and President, Whitehawk

Dr. Dimitri Kusnezov, Chief Scientist, National Nuclear Security Administration, Department of Energy (DOE), USA

15:00 - 16:00 4TH SESSION: CYBER IN MOTION

Chair: **Matan Scharf,** Strategic Advisor, Blavatnik ICRC; Cyber Security Specialist, Researcher and Entrepreneur

Esti Peshin, Director of the Cyber Programs, Israeli Aerospace Industries

Arik Mimran, General Manager, Vice President of Engineering, Qualcomm

Chris Roberts, CSH and Senior Consultant, Sentinel Global.

China-Israel Academic Cooperation Roundtable

Sunday, June 19th, 2016, 13:00 – 14:30
Room 527 Venezuela Hall, Naftali Building, TAU

Participants:

Prof. Joseph Klafter, President, Tel Aviv University
Major Gen. (Ret.) Prof. Isaac Ben-Israel, Director, Blavatnik Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University
Prof. Yehuda Afek, Professor of Computer Science, Blavatnik School of Computer Science & Researcher, Blavatnik ICRC, Tel Aviv University
Lior Tabansky, Cyber Power Scholar, The Blavatnik Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University
Zhao ZeLiang, Director General, Bureau of Cyber Security, China
Liu Chang, Research Fellow, China Internet Network Information Center, China
Huang Renqiang, Deputy Director, Internet News Research Center, Cyberspace Administration of China
Prof. Cheng XingShun, Executive President, SiChuan University, China
Prof. Li Hui, Executive Vice President, Xidian University, China
Huang Yonghong, Deputy Director General, Cyberspace Administration, Shaanxi Province
Li Jun, President, Sugon Information Industry Co. Ltd
Lin YongJun, President, Beijing E-hualu Information Tech Co. Ltd.
Pan ZhongYu, Vice President, Beijing Venustech Inc.
Wong King, General Manager, EcGuard

Cyber Horse 2016

The Cyber Horse is a piece of work created with thousands of infected computer and cell phone components.

It illustrates the increasing use of malware in making cyberspace a hostile environment.

Like in the legendary story of Troy, the Cyber Horse stands at the front gates of the Tel-Aviv cyber conference auditorium.

Like its namesake, it conceals bad news and is waiting for the doors to open.

Will it stream inside, or will the conference participants block it?

Idea, design, & installation

No,No,No,No,No,Yes®

Italy-Israel Workshop

Tuesday, June 21st, 2016, 16:00-19:00
Room 003, Naftali Building, TAU

Opening Remarks:
Professor Isaac Ben Israel, Director of the Blavatnik ICRC

Presenters:
Joint Research: Mr. Franceso Moro, Researcher Fellow at the University of Milano-Bicocca, Adjunct Professor at LUISS University, Rome & **Mr. Lior Tabansky,** Cybersecurity Policy Expert, Researcher at the Blavatnik ICRC
Professor Joachim Meyer, Department of Industrial Engineering, Researcher at the Blavatnik Interdisciplinary Cyber Research Center
Professor Bruno Crispo, Professor of Information Engineering & Computer Science at the University of Trento
Professor Nathan Intrator, Professor of Computer Science & Neuroscience at Tel Aviv University, Researcher at the Blavatnik ICRC
Mr. Mirco Marchetti, Research Fellow of the University of Modena and Reggio Emilia
Professor Avishai Wool, Deputy Director of the Blavatnik ICRC, Associate Professor of Electrical Engineering at Tel Aviv University - Anomaly detection in in-vehicle CAN Bus Networks
Dr. Stefano Boccaletti, Researcher at the National Research Council and Scientific Attaché of the Italian Embassy in Israel
Closing Remarks:
Professor Isaac Ben Israel, Director of the Blavatnik ICRC
Professor Michele Colajanni, Professor of the University of Modena and Reggio Emilia, Director of the IL-IT CyberLab
Dr. Gianfranco Incarnato, Italian diplomat since 1985 at UN, EU and NATO; Central Director for security, cybersecurity and disarmament.

UK-Israel Roundtable

The event is held in conjunction with the UK-Israel Tech Hub, British Embassy Israel

Tuesday, June 21st, 2016, 16:30 – 18:00
Venezuela Hall, Room 527, Naftali Building, TAU

This is a unique roundtable hosted by the UK and Israel. Join as innovative cybersecurity leaders discuss various elements within the cyber ecosystem and strengthen relations between the two countries. The dialogue will focus on the exchange of knowledge and information, the importance of investing in human capital, IP restrictions, cyber incubators and much more.

Moderator:
Roni Zehavi, CEO, Cyberspark
Participants:
Dr. Ian Levy, Technical Director of the new National Cyber Security Centre
Paddy Davy, International Cooperation, NCSC.
Yoav Tzruya, JVP
Ilan Graicer, Strategic Advisor to the ICRC and Cyber Insecurity Specialist
Menny Barzilay, ICRC and CEO, FortyTwo
Mr. Niv David, Lecturer and Research Fellow, Cyber & Tech Operations, ICRC

UK Israel Tech HUB

Cyber-Insurance Roundtable:

Cyber Technology meets Cyber Insurance

Wednesday, June 22nd, 2016, 16:00 – 19:00
Room 106, The Porter Building, TAU

Presentations from:

Mr. Jacob Mendel, Head of research cooperation with the industries, ICRC, General Manager Cyber Security COE, Intel
Mr. Shay Simkin, Managing Director of Howden Insurance Brokers Israel, Head of Cyber for Howden Global
Mr. Yoram Golandsky, CEO, CybeRisk
Mr. Graeme Newman, Chief Innovation Officer, CFC Underwriting
Mr. Ryan Jones, Director of Cyber Risk Intelligence, BMS
Ms. Philippa Berry, Technology and Cyber, Aspen Insurance
Mr. Daniel Garrie, Head of Cyber Security Practice, Zeichner Ellman and Krause
Mr. Ori Eisen, Founder & CEO, Trusona

Annual Youth Conference

Sunday, June 19th, 2016, 10:00 – 13:00
Bar-Shira Auditorium, TAU

TOMORROW'S CYBER LEADERS

The conference will include presentations from leaders in the industry, such as:

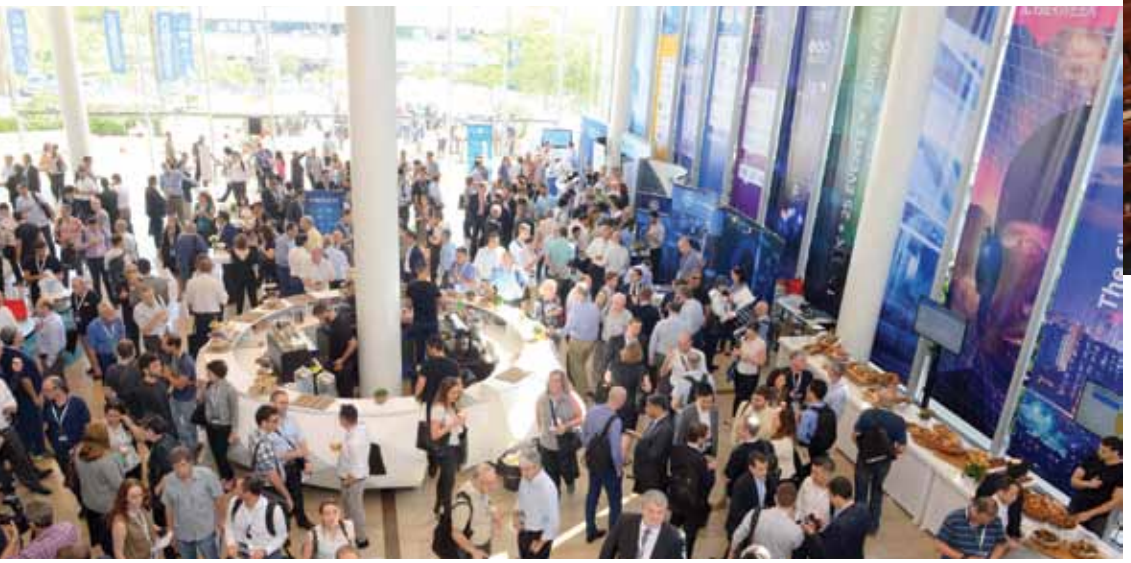
- **Nadav Zafrir,** Co-Founder and CEO, Team8
- **Yanki Margalit,** Social entrepreneur, investor and Chairman, SpaceIL
- **Menny Barzilay,** Strategic Advisor at the Blavatnik ICRC and CEO, FortyTwo Israel
- **Michael Shaulov,** Head of Mobility Product Management, Check Point Software Technologies
- **Adi Stein,** Founder & CEO, FitUup

* This event is closed for registration. It is dedicated for young students from science and cyber programs only.

THE ROAD AHEAD

The ICRC has already earned acclaim as a large, cross-disciplinary, vibrant center. The Cyber Week and supported research have already achieved significant sustained impact. These core activities will continue to mature, supplemented by new steps. In the near future, the ICRC will commence several endeavors to further extend the volume and intensify the quality of cyber research.

Notwithstanding operating for up to two years, the research teams supported in the 2014-2015 CFP have already presented research in prestigious conferences worldwide, and already submitted dozens of scientific articles to the leading academic journals in each discipline.



POSTDOCS EXCHANGE

The ICRC will develop programs and projects to accommodate foreign postdocs from the leading universities worldwide in TAU for significant periods to conduct meaningful research and teaching.

The ICRC will develop mechanisms for TAU graduate student and postdocs exchange in the leading universities worldwide.

INDUSTRY PARTNERHIPS

The ICRC welcomes partnerships with the industry for training, research, education, and welcomes sponsors.
The ICRC will develop programs and projects to enhance industry-academia relations, including with leading multinationals.
The ICRC will strive to leverage existing institutionalized mechanisms for industry-academia cooperation, including the relevant programs in EU Horizon 2020.
The ICRC will initiate review and updating of selected teaching curricula using data and case studies from industry.

EDUCATION TIES

The ICRC will initiate relations with individual schools and offer support in designing cutting edge programs, that will increase cyber literacy as well as grow future innovators. These ties shall also contribute to increased pupils desire to pursue academic studies in TAU.

GRANTS AWARDED 2014-2016

RESEARCH ABSTRACTS

Listed in alphabetical order

The Blavatnik ICRC has awarded grants to 56 winning teams, selected from 101 proposals between 2014-2016

RESEARCH ABSTRACTS OF CFP WINNERS

Listed in alphabetical order

ADAPTING QUANTUM CLUSTERING (QC) AND RELATED ALGORITHMS TO ANOMALY DETECTION IN BIG DATA

DAVID HORN

Quantum clustering (QC) is a successful clustering algorithm. One version of it (DQC) has already proved its ability to detect anomalies in big data. We review these successes and propose to extend the algorithm, within a novel entropy formulation, to three different methods. We propose to adapt them to big data, thus allowing for their application to problems relevant to cyber security. We also propose to employ them within Deep Neural Networks as novel exploratory tools. We plan to test our methodology within various domains, including speech processing, financial fraud and malware.

Work Plan:

Develop the Entropy analysis and clustering tools.

- Apply the algorithms to various scientific and technical problems to gain further insights into the strengths of the different schemes.
- Develop an approximation method, first discussed in ref. 5, in order to enable fast and accurate calculations of replica dynamics.
- Use the approximation for carrying out applications to big data.
- Search in big data for string-like structures of the type uncovered by DQC analyses.

Incorporate Clustering in Deep Neural Networks.

- Improve the performance of DNN on big data
- Explore for the existence of clusters with unexpected characteristics

Use different data sets such as:

- Speech processing (in collaboration with an expert team in Afeka college)
- Financial fraud data (possible connection with Citibank)
- Malware and fraud data (collaboration with an expert team in EMC)
- Israeli CERT data, as well as cyber security data from public resources such as www.predict.org.

ADVANCED ATTACKS AGAINST INTERNET SECURITY PROTOCOLS

YUVAL SHAVITT

We have recently presented DROWN, 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 have presented two versions of the attack. The more general form exploits a combination of thus-far unnoticed protocol flaws in SSLv2 to develop a new and stronger variant of the Bleichenbacher attack. A typical scenario requires the attacker to observe 1,000 TLS handshakes, then initiate 40,000 SSLv2 connections and perform 250 offline work to decrypt a 2048-bit RSA TLS ciphertext. (The victim client never initiates SSLv2 connections.) We have implemented the attack and can decrypt a TLS 1.2 handshake using 2048-bit RSA in under 8 hours using Amazon EC2, at a cost of $440. Using Internet-wide scans, we have found that 33% of all HTTPS servers and 22% of those with browser-trusted certificates are vulnerable to this protocol-level attack, due to widespread key and certificate reuse. For an even cheaper attack, we have applied our new techniques together with a newly discovered vulnerability in OpenSSL that was present in releases from 1998 to early 2015. Given an unpatched SSLv2 server to use as an oracle, we can decrypt a TLS ciphertext in one minute on a single CPU - fast enough to enable man-in-the-middle attacks against modern browsers. 26% of HTTPS servers are vulnerable to this attack.

We have further observed that the QUIC protocol is vulnerable to a variant of our attack that allows an attacker to impersonate a server indefinitely after performing as few as 2^{25} SSLv2 connections and 2^{65} offline work. We have concluded that SSLv2 is not only weak, but actively harmful to the TLS ecosystem.

DROWN was covered by, among others, The Guardian, Forbes, and the BBC. We have responsibly disclosed the attack in advance to the Israeli National Cyber Bureau. **We now seek to extend the attack to directly target modern cryptographic protocols**, even without the presence of a shared RSA key exposed using an obsolete protocol. Worryingly, TLS and similar modern protocols exhibit properties that were used in DROWN, thereby giving us cause for hope, or rather worry, that they can also be targeted directly using this approach. DROWN is in fact the first project to present and formalize the properties which make a protocol vulnerable to a direct-message side-channel Bleichenbacher attack.

Workplan

- Improved anti-Bleichenbacher countermeasure
- More classic Bleichenbacher attacks
- New accelerated handshake mechanism in the Fiat-Shamir model
- New attack against TLS

With those tools in hand, we will try to mount new attacks against modern cryptographic protocols, especially TLS, using the approach in, is significantly different from classical Bleichenbacher attacks.

ANOMALY DETECTION FOR CRITICAL INFRASTRUCTURE PROTECTION: SECOND GENERATION

AMIR AVERBUCH

Several factors make anomaly detection in high dimensional big data (HDBD) a challenging task: learning HDBD distributions, the boundary between normal and abnormal behavior is sometimes vague, many scenarios exhibit data that evolve in time which means that what is currently considered as a normal behavior might be abnormal in future and vice versa and there is a need to employ many different domain experts. This may cause high false alarms rate. In this proposal, we focus on an automatic and unsupervised anomaly detection in an unstructured HDBD that do not necessitate domain expertise, signatures, rules, patterns or semantics understanding of the features and propose several new methodologies for anomaly detection for protecting critical infrastructures. Anomalies can originate from either a cyber-attack/threat or operational malfunction, or both. The proposal shows that those can be detected simultaneously even though the data sources leveraged for each case can be entirely distinct. We also show that cyber threat and operational malfunction are converging into a single detection paradigm.

Why there is a problem: The basic approach in securing critical infrastructures in the past 45 years, classified as "walls and gates", has failed.

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. This will be accomplished from our understanding massive amounts of data by designing unsupervised learning algorithms, that "understand/quantify" and model complex topics/contexts that extract critical intelligence from data to uncover unprecedented unknown unknowns (anomalies = threats, operational malfunction, trends). This proposal can be considered as part of the **Industrial Internet** initiative, which is a subset of **Internet of Things**. HDBD can be described by hundreds or even thousands of parameters (features). Anomaly detection identifies patterns in a given HDBD that do not conform to an established/expected normal behavior baseline. The detected patterns, which deviate from normality, are called "anomalies".

We propose a methodology blending tools from multidisciplinary approaches such as applied and computational harmonic analysis, stochastic processing (random walk, Brownian motion), randomized algorithms, differential geometry, classical analysis, geometric measure theory, manifold learning, low rank matrix decomposition, spectral graphs, kernel methods and dictionary constructions that are versatile to process efficiently HDBD. The goal is to turn data into quantitative knowledge. The availability of massive data is a huge opportunity for us since we can understand, process, manipulate and extract actionable intelligence from it.

The proposed algorithms are generic and the same core underlying infrastructure can be used to perform a general anomaly detection for various tasks such as performance monitoring and analysis, unified threat manager for network health, smart phone protection, risk management in diverse financial transactions, fraud detection, prediction and tracking of emerging problems and problem avoidance.

The research builds upon our First Generation anomaly detection methodologies, which were developed in the last 7 years, have used diffusion geometry of HDBD for manifold learning to detect cyber based anomalies in structured HDBD, and published in 26 papers.

ANONYMOUS AND SECURE ELECTRONIC VOTING: PROTECTING OUR DEMOCRATIC INFRASTRUCTURE

AMNON TA-SHMA, ALON ROSEN

In the last decade, there have been several attempts in Europe and the US to move from paper-based voting to electronic voting. Many of these attempts have failed. A recent study on Estonia's Internet electronic voting system reports: **"What we found alarmed us. There were staggering gaps in procedural and operational security, and the architecture of the system leaves it open to cyberattacks from foreign powers, such as Russia. These attacks could alter votes or leave election outcomes in dispute. We have confirmed these attacks in our lab - they are real threats. We urgently recommend that Estonia discontinue use of the system."**

We wish to design and implement a working system that is both practical and secure, and make it available to testing by researchers in Israel and abroad. The core of the problem with electronic voting is that often the integrity of the whole election relies on the correct functioning of the electronic equipment. However, in reality, one cannot trust any part of the system, be it hardware or software, and the challenge is to devise a cryptographic protocol that enables the verification of the correct functionality of a complicated, digital system, where the verification has to be made by a human being. This situation has led to the introduction of the notion of "software independence". A voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome. Several software-independent cryptographic protocols were suggested, including Pret-a-vote, Punchscan and Scantegrity. Scantegrity II was used in the Takoma Park municipal elections in Novemeber 2008. We wish to implement a dual voting system, combining cryptographic and paper election, that combines the flavor of traditional paper based systems, while guaranteeing all the advantages of cryptographic electronic voting. We believe the transition to electronic voting is inevitable, and that there is no alternative to software-independent voting. In this research, we will study the delicate security issues involving electronic voting and will implement and test such a system.

ATTACK RESILIENT RESOURCE PLACEMENT IN CLOUD COMPUTING SYSTEM AND POWER GRID

HANOCH LEVY, ELI BROSH (CANARY CONNECT), GIL ZUSSMAN (COLUMBIA UNIVERSITY)

Distributed data centers (that provide cloud based services) and power grids are key infrastructure systems whose resilience to cyber (and physical) attacks is of utmost importance. In particular, failures in these systems can have devastating impacts on various interdependent military and civilian systems (e.g., communications, gas and water supply, and transportation). Hence, in this project, **we will focus on resource allocation in cloud computing and power grids that accounts for failures resulting from attacks and for highly variable demands**.

Resource allocation schemes for these geographically distributed systems should support mitigating the impacts of potential cyber attacks while maintaining the required level of service during regular operation. **However, designing such schemes poses major challenges due to the high-dimensionality of the problems and the special characteristics of the flows in power grids. Addressing these challenges requires an interdisciplinary approach that employs methods and techniques from various areas, including stochastic control, power flow optimization, and algorithm design.** Specifically, we will consider the general problem of resource allocation in a geographically distributed system, where resources have to be allocated for m types of services in n geographical locations. The allocation is based on a known *stochastic* demand for the services (mxn dimensional) and on the costs of providing the services from different locations. Under this general setting, we will address the two following problems: **Cloud services under attack and Power grids under attack. We will extend the methodology we previously developed that provided very efficient solutions to a wide variety of these problems in non-hostile environments,** and devise algorithmic solutions which will provide resource placement strategies that will be efficient/optimal with respect to malicious environments. We will build on this methodology and tailor it to the special challenges posed by hostile environments and

power grids. In the context of **cloud computing**, we will capture the volatility of the resources due to attacks by modeling the resources, namely the 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 our previous work, the 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. We expect the analysis to 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, level of service in regular operation, and cost.

A very important variant of this problem arises when **there is a need to accommodate mutually hostile resources.** This need arises when security-aware clients require that their resources are (physically or logically) isolated from other resources (e.g., commercial or government entities concerned with data leakage between cloud tenants and espionage on their data, and defense or public safety organizations that need to separate confidential and non-confidential services). The service provider can, for example, grant secure service using geographic isolation (i.e., place the services of mutually-hostile organizations in separate data centers). Such separation, however, will inflict operational costs. These costs can be incorporated in our framework, where remote service costs more than local service (see toy problem). We plan to use our methodology to develop optimal and approximate attack resilient placement algorithms that satisfy the separation requirements.

In the context of the **power grid**, we will focus on cyber attacks that have a physical impact (e.g., shutting down a generator or faulting a power line). We will study the design problem of placing resources (e.g., generators and additional power lines) in a manner that can provide attack resiliency. This will require combining the methodology, described above, that takes into account stochastic supply (due to failures) with the DC approximation of the power flow [1] that allows evaluating the effects of changes in supply and demand. To better understand the design problem, we will also study the cascade control problem in which there is a need to halt a cascade that is initiated by an attack on some of the allocated resources. Finally, we plan to develop resource allocation algorithms that take into account the dependency between the grid and the cloud, where due to an attack on the grid and loss of power, cloud resources become unavailable.

AVIONIC BUS CYBER ATTACK IDENTIFICATION

AVISHAI WOOL, GABI SHUGUL (ASTRONAUTICS C. A. LTD), RAZ TIKOCHINSKI (ASTRONAUTICS C. A. LTD)

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.

Existing avionics are based on system architectures dated 10-25 years back, and lack the required cyber protection of today's computing world. For years the concept of the avionics system designer was based on the fact that the avionics are not connected to the IT world and networks; therefore, it does not require special protection against threats from the outside world. However, avionics systems have evolved and currently include Ethernet buses, connected to many systems, either wired or wirelessly, including data-link and satellite communication data exchanges, modernized data and software loading via maintenance loaders and even modern wireless data links to the ground. Therefore, cyber security measures are required throughout the entire chain – from the maintenance repair shops and up to the aircraft, with means to detect and block any cyber threat while loading data, but also onboard, detecting and protecting any cyber threat that is already resident within the avionics and may damage the system or its' operational use. We focus on the most common military avionic bus, known as the MIL-STD-1553B bus. This bus is the main communications bus onboard military aircraft, used as the major data exchange vehicle for all military avionics systems (total existing

worldwide military aircraft fleet using this type of bus is estimated to be close to 50,000 aircraft).

The research hypothesis is that the characteristics of the low-level electrical signals generated by the various bus elements are unique, and can be used to reliably identify the transmitting element, independently from any protocol-level information regarding the identity of a message source. The scope of the research is to evaluate this hypothesis, by developing a "fingerprint" for each of the devices connected to the bus based on normative electrical and timing behavior of each device, and to evaluate the fingerprint's performance. Specifically, Astronautics would like to take an initial concept of analyzing the electrical characteristics of the MIL-STD-1553B bus, and establishing an electronic "fingerprint" for each of the devices connected to the bus, helping to identify anomalies in the bus "behavior" that will indicate a possible cyber attack. A successful outcome of this research will allow us to detect different kinds of spoofing cyber attacks and misuse of the bus by malicious devices. To the best of our knowledge, no existing MIL-STD-1553 cyber attack detection currently exists. Astronautics' avionics cyber lab enables the creation of various attack vectors, evaluating their impact on avionic systems, before and after implementing various detection and protection algorithms. Thus, Astronautics' cyber lab shall support the development and implementation of cyber security solutions, and will allow testing of these solutions' effectiveness in various scenarios. Astronautics will develop the MIL-STD-1553B bus front end high frequency sampling device for digitizing the signals and will build the environment of the bus, devices and cyber attack demonstrations. Prof. Wool and his students will develop the algorithms to study the fingerprints and detect bus anomalies.

BALANCING NATIONAL SECURITY AND PRIVACY RIGHTS TO PRIVACY AND THE RULE OF LAW IN DEMOCRATIC SOCIETIES A COMPARATIVE ANALYSIS

DEBORAH HOUSEN-COURIEL

One of the most compelling challenges facing democratic societies at present is that of achieving the appropriate balance between national security considerations and citizens' rights to privacy in cyberspace. The challenge is an old-new one. Calibrating the necessary security-privacy balance was also an ongoing challenge in the pre-internet era, as the principle of individual privacy was weighed on an ongoing basis against the security priorities of government agencies in a variety of contexts. Specifically, the traditional, pre-cyberspace categories of privacy addressed three principles: (1) limiting government surveillance of citizens and use of data about them, (2) restricting access to certain types of data, such as personal data, and (3) limiting entry into places deemed private. These principles address the challenges of privacy protection in cyberspace as well, but must now be applied in the context of state and private activity in cyberspace – in circumstances that are unfamiliar and unanticipated. Two key events that have so far sharpened governments' awareness of what is at stake in terms of national security, and the extent to which their data gathering is a two-edged sword, are the release of sensitive government data by Assange in 2010 and by Snowden in 2013.

The "choices as a society" between security and civil liberties are the focus of this interdisciplinary research. On the one hand, national security considerations are crucial to the physical survival, the rule of law and the social integrity of modern democracies. On the other, the widespread violation of personal and institutional privacy on the part of security organizations such as that carried out by the US' NSA and other national security bodies in Western democracies, through their past monitoring of private communications is intolerable to many citizens in these same democracies.

Analysis of the legal frameworks in place is not sufficient to give a full picture of the current dilemmas around the national security- privacy tensions in contemporary democracies, although the legal regimes will serve to anchor

the overall analysis. The interdisciplinary nature of the research compels investigation of additional elements: public policy approaches, the definitions of "data" and examination of its attributes and their ramifications, and extra-legal approaches to the concept of individual privacy in contemporary democracies. The exploratory nature of the research at this point in time is emphasized, as is the aim of informing the professional debate in Israel about this crucial cybersecurity issue. The study will explore four national models of the national security – privacy balance (the US, UK, Australia and Israel). Its aim will be to elicit those elements of balancing in the four regimes studied that may be useful in thinking about future legal and regulatory regimes, in Israel in particular. An end result is envisaged of enriching the public and professional debate in Israel and in other countries around the national security-privacy issue.

BEST PRACTICES FOR VERIFIABLY-CORRECT CONCURRENT SYSTEMS

NOAM RINETZKY, SHARON SHOHAM

Concurrent software systems play a vital role in our life. Unfortunately, they are known to be difficult to design, implement, debug, and verify: The tremendous number of potential interactions between concurrently executing threads leads to scenarios which defy human intuition. The growing dependence of modern society on software systems calls for more rigorous techniques for ensuring correctness of concurrent systems.

The goal of the proposed research is to change the current unsatisfactory state of affairs. Specifically, we will provide formal, implementation-independent, definition of best-practices for constructing concurrent systems, and design tools that can either *verify* that a given concurrent module adheres to the desired best-practice or *synthesize* a concurrent module which respects an intended correctness condition in a provably correct manner.

Success criteria. We aim to develop our techniques so they can be applied to real-life systems. Thus, we will measure our success by the scale of the systems for which they can be applied. By scale, we do not mean the number of lines of code in the system, but the complexity of its concurrency control mechanism. In particular, the success of this project will be measured by the ability of the tools it will provide to specify/verify/synthesize interesting concurrent modules which cannot be handled by current state-of-the-art formal techniques.

An ideal outcome of our project would be a "cookbook" which a programmer wishing to build a concurrent module satisfying a certain correctness condition, e.g., serializability, using a particular synchronization mechanism, e.g., optimistic locking, could open, and find a formal definition of a policy which she should follow, together with a verification technique that could determine if she implemented the practice correctly, or even a mechanism that would allow her to synthesize a correct implementation out of a sequential module. However, achieving such a result would require far more resources than we can ask for. Thus, we plan to focus our work by selecting a few correctness conditions, e.g., serializability, linearizability, and opacity, and address the three aforementioned challenges with these conditions in mind, but place the particular emphasis on the specification and verification aspects of the project. The selection of the particular conditions will be directed by the practical test cases that we will review at the beginning of the research. We believe that even if we limit ourselves to a few correctness conditions, the techniques and approaches that we will develop will inspire and enable other researchers to follow a similar research program, but targeting different condition. Furthermore, as the conditions that we will handle will be ones the we find in real-life applications, our results would help programmer construct safe and secure practical concurrent systems.

CO-LOCATION-RESISTANT CLOUDS SECURITY

YOSSI AZAR

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 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 connections 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.

In a recent work, we consider the problem of cross-VM attacks in public clouds, seeking solutions that do not rely on single-tenancy or on systems-level assumptions. At a very high-level, our focus is on mitigating co-location attacks since they are a necessary first step to performing cross-VM attacks. More concretely, our approach is to assign VMs to physical servers in such a way that attack VMs are rarely co-located with target VMs. To do this, we formalize and design co-location-resistant placement algorithms which, roughly speaking, protect VMs against complete and fractional co-location attacks. Our main placement algorithm uses randomization to place VMs in a manner that is unpredictable to the adversary and that reduces its probability of successfully completing a co-location attack. We note that the naive strategy of placing VMs on servers chosen uniformly at random is not feasible in our setting since VMs cannot be placed arbitrarily in practice. Indeed, VM placement algorithms have to satisfy non-trivial optimization constraints which cannot be met by simply placing VMs at random. One of the major contributions of our work is the design of an algorithm that optimizes for these constraints while remaining co-location-resistant to the adversary.

Secure optimization. As far as we know, ours is the first work to consider the design of such "secure optimization" algorithms; that is, optimization algorithms that also provide some form of security. We believe the study of secure optimization algorithms is an interesting research direction at the intersection of algorithms, security and cryptography and could have applications, not only to cloud computing, but more generally to distributed systems.

Combining cryptography with security. Another major contribution of our work is combining cryptography with security and suggest our notion of shared deployments. Specifically, we show how to take advantage of complete and fractional co-location-resistance through the use of cryptography. At a high-level, our approach is to assume the adversary is computationally-bounded and to cryptographically "split" a tenant's computation among a set of VMs in such a way that the tenant's secrets can only be recovered if the adversary co-locates with all the VMs in the set. This allows us to provably improve the quality of the system security.

CONFESS OR DENY? STRATEGIES FOR DEALING WITH CYBER ATTACKS

DEGANIT PAIKOWSKY, GIL BARAM

The manner in which a nation-state reacts to a cyber-attack, both domestically and internationally, is significant. In light of the unique characteristics of cyber operations and the growth of their frequency, there is an intensified need for discussion regarding the efficacy of policies and practices to manage reactions to cyber-attacks. The proposed research investigates the preferred strategy for attacked nation-states in admitting or hiding an attack. The research focuses primarily on democracies, in which public transparency holds a significant value, which serves the overall interests of society and its government. In contrast, unreliable official announcements, intended to hide and cover an attack, can lead to constant suspicion towards governmental systems and

public officials. On the other hand, one cannot discount the fact that hiding an attack may serve specific national security objectives.
In open and democratic societies, over time, public mistrust may develop when actual attacks are being covered up as technical malfunctions. This loss of public trust may have severe consequences and long-term effects on national security.
We argue that an admission of a cyber-attack may promote transparency and generate public confidence in the governmental system; neither of which should be ignored as they hold significant value, especially in a democracy. Nation-states often avoid admitting they had been attacked, making such case studies a rare phenomenon. Therefore, theoretical scenarios will be used in the theoretical discussions in order to illustrate the dilemmas and allow for the discussion of the various considerations that said nation-states should take into account.

COMPILATION INTEGRITY ASSURANCE THROUGH DEEP CODE ALIGNMENT

LIOR WOLF

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. Consider, as an accessible example, the compilation of firmware that is provided by the hardware designer as C code and is compiled at the foundry. 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 apply the novel tools we propose in order to 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. The detection of hardware Trojans is almost impossible post manufacturing: modern ICs have millions of nodes and billions of possible states, high system complexity, and are of a nano-scale. Besides, it is very difficult for unknown threats, for which no signatures exist and which are triggered at very low probability. Inserting malicious code as part of the compilation process done at the foundry is relatively easy and is very hard to prevent. While there are other means for inserting hardware Trojans, none are as cheap and straightforward. Verification of the compilation process is therefore of an immense importance.
Most facilities of advanced ICs fabrication and electronics assembly have migrated offshore due to economic pressure. This move has been accompanied by the dominance of the fabless model, in which the thousands of electronics manufacturing services suppliers hand over control of their design to two dozen foundries, mostly in the far east. Trust cannot be guaranteed in this model. The few remaining suppliers that keep using IDM model, where fabrication is done internally, can no longer provide the performance and variety of ICs that are needed. Therefore, establishing trust as part of the hardware manufacturing process is expected to become more and more critical and the tools developed in this project could be adopted very quickly into IC fabrication and firmware compilation. In addition to Trojan detection, the tools we are developing would support and automate a wide range of code analysis tasks that are currently being handled by a large number of engineers working for defense agencies. By building on the tools to be developed and modifying them, e.g., to align binary code with recompiled binary code, one can solve, for example, the task of analyzing executables as these shift from one version to the next, and the analysis of electronic devices as models are being replaced.

We address the task of statement-by-statement alignment of source code and the compiled object code. An explicit approach to this alignment problem is infeasible since the complexity of directly modeling it approaches the one of building the compiler itself, and needs to be done per-compiler. Instead, we propose to employ a deep neural network, which maps each statement to a context-dependent representation vector and then compares such vectors across the two code domains: source and object.

CRIME AND IOT

ROEY TZEZANA

Capabilities that were considered 'science fiction' a mere few years ago, become usable in the hands of individual criminals and crime organizations in the present. It is therefore vital to consider future possible cyber-crimes in advance, even before they become feasible. Internet of Things (IoT) will have a large impact on our lives by tapping into information sources about our day-to-day doings, and providing common items with the basic intelligence needed to impact our lives in turn. While the potential benefits are great, there is also a vast and fertile ground for using the IoT to enact novel crimes – from burglary to fraud to identity theft and other types of crime. We suggest developing a better understanding of the security measures and regulations needed to combat the 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 with policy advice on how to prepare for said crimes. The Israeli Police Department of Strategic Planning has agreed to act as a stakeholder and to collaborate in this research.

Research Plan

Literature review about the IoT and the security of smart cities.

Obtaining parameters and values for potential crimes: using brainstorming workshops and expert surveys, we will identify the many different parameters and values of future possible crimes. Parameters could include the identity of the criminal (and the values for that parameter could be individual or crime organization, for example), the type of crime (the values for which will include murder, burglary, rape, etc.), technologies used to enact the crimes, the earliest date for feasible use, etc.

Cross-linking the values: the links between certain values will be identified with the help of experts, so that we can understand which technologies can best be used for which types of crimes, and how technologies can be used together to create crimes with a higher damage-potential.

Identifying high-damage potential combinations of values: high-damage potential combinations of values will be identified, using an algorithmic customized approach (General Temporal Morphological Analysis).

Scenario development: scenarios will be developed for each high-damage potential combination of values.

Policy generation: the scenarios will be presented in a workshop, and policy and strategy advice will be obtained from the participants regarding the ways in which the regulator and the police can become better prepared to those scenarios.

Final report: the full results of the research, including the identified parameters and values related to future crimes, their potential combinations, the selected scenarios and policy advice, will be published in a final report that will be submitted to all the relevant governmental offices, law-enforcement bodies and international organizations that deal with similar issues.

CYBER JIHAD TAXONOMY: QUALITATIVE ANALYSIS OF THE BEHAVIOR OF JIHADI MEMBERS ON SOCIAL NETWORKS AND THE JIHAD SUBCULTURE THEY CREATE

UDI SOMMER, GAHL SILVERMAN (BAR-ILAN UNIVERSITY)

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. 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.

Objectives of the Proposed Project

What are the characteristics of a potential Jihadi extremist as reflected in SNS discourse? This study has three main goals:

1) To identify the characteristics of a potential Jihadi terrorist;
2) To identify the taxonomy of the discourse between Jihadi members on SNS; and,
3) To create a categorization of posts and replies that exhibit or inspire an implied preliminary jihadi terrorist behavior.

Methodology

This study will zoom in on the individual level and make a multilayered picture of cyber jihad subculture. We will employ a mixed methods analysis software (NVivo11), using a two stage inquiry to analyze posts and related replies. At the first stage, we will focus on a selected sample of posts and replies that contain Jihadi discourse through text, audio and video, in English and possibly in Arabic. Classification, discourse, conversation and semiotic analysis will be applied to study each post and related replies independently. At the second stage, Lexical Identifier Mapping, based on content analysis methodology, will be applied to group relevant posts and related replies based on content similarity.

CYBER INFORMATION SHARING IN A COMPETITIVE AND CONFLICTED ENVIRONMENT

AVIRAM ZRAHIA

Innovative cyber-attack methods, collectively referred to as Advanced Persistent Threat (APT), reduce the effectiveness of traditional security mechanisms. In turn, emerging defense technologies, such as dynamic threat feeds, leverage upon the sharing of cyber information with outside parties to address these cyber vulnerabilities. Whether it is valuable to share cyber information in a competitive business environment is still not well understood. In the proposed research, I will study the dynamics of threat information sharing between competitive security vendors.

Cyber information-sharing is the communication of relevant information among separate organizations in a collaborative effort to improve cyber defense postures by leveraging the capabilities, knowledge, and experience of the broader community. In recent years, a number of sharing alliances have emerged: between organizations, within the same vertical market, across sectors, between commercial and government bodies, and even between countries. The challenge of information sharing increases when the parties are direct competitors or have other conflicts of interests. The sharing entities need to maintain their competitive edge and comply with anti-trust laws and regulations, while providing a meaningful amount of high-quality shared data to make the alliance useful.

Whereas cyber security information sharing can easily be justified for vertical markets outside of the cyber security industry, the value of cooperation among competing cyber security vendors is less obvious. The proposed research focuses on the latter kind of cyber alliance.

The goal is to study the dynamics of threat information sharing among security vendors, by applying academic theory into the problem domain. The research will answer the following question: what drives certain security vendors to share threat information with competitive parties, and what are the sharing structures.

The research will use the following theoretical constructs: (1) information sharing – studies the financial impact of sharing on organizations, and (2) coopetition – a framework used in the business literature to evaluate cooperation among business competitors. This empirical research incorporates academic theories into the cyber threat information sharing landscape in the following methodology: use concepts from the literature to form hypotheses on the factors influencing the sharing decision of a security vendor, collect financial and other data variables relevant to the factors suggested on a large list of security vendors, and use statistical and other tools to check the hypotheses and point out the significant variables impacting the sharing decision, and the alliance structures.

CYBER, SPACE AND NUCLEAR WEAPONS ANALOGIES, INTERRELATIONS AND DIFFERENCES IN FORMING NATIONAL STRATEGY – A COMPARATIVE ANALYSIS OF THE UNITED STATES AND RUSSIA (USSR)

AMIR LUPOVICI, DEGANIT PAIKOWSKY, OR RABINOWITZ (HUJI), DIMITRY (DIMA) ADAMSKY (IDC HERZLIYA)

The research will explore and compare the evolution of American and Soviet/Russian strategic thinking by examining how the layered development of Nuclear, Space and Cyber capabilities impacted the development of concepts of national security in these countries.

Our main goal is to map the interrelations among cyber, space, and nuclear weapons in American and Soviet/Russian strategic thinking on the one hand and the differences among the strategic thinking regarding these technologies on the other. Toward these goals, at the first stage we seek to develop key points of categorization and comparison that will allow us to better understand how each technology affected these countries national security thinking. At the second stage, we will apply this knowledge in order to trace the differences, analogies and interrelations among these technologies in forming strategic thinking.

CYBER SECURITY TECHNOLOGY FORESIGHT

TAL SOFFER

The research questions of the study are:

1. What are the main cyber threats that industrial control systems face today?
2. Which technologies and methods are being used at present to secure industrial control systems from cyber attacks?
3. What are the main cyber threats that industrial control systems will face in the next 10-15 years?
4. Which emerging and future technologies will be used to secure industrial control systems in the next 10-15 years?

The main goal of the study is to derive the current cyber security technology status from the analysis of popular standards such as NERC-CIP. Based on this mapping, a foresight process will be carried out in order to assess future directions and emerging technologies in cyber security. The process will include horizon scanning, analysis of key technologies and drivers, scenarios development, expert surveys and recommendations.

The expected outcomes of the project:

1. State of the art cyber security standards
2. Horizon scanning of trends and megatrends that are relevant to cyber security
3. Analysis of future and emerging technologies that are important to cyber security
4. The most important drivers impacting the cyber security industry
5. Expert survey to assess and determine the most promising emerging technologies including their impact and time to market
6. Recommendations for cyber security R&D policy
7. Peer reviewed paper including the results of the projects

CYBER THREATS IN SELF-REGULATING DIGITAL PLATFORMS

OHAD BARZILAY, GAL OESTREICHER-SINGER, HILAH GEVA

Alongside the benefits of allowing computers to regulate systems, some risks arise. Computer algorithms may be susceptible to errors and manipulation. They may overlook corner cases and serendipities that they are not wired to detect, and they lack the "common sense" for "doing the right thing" in situations that are not covered by their cookbooks. Given the pros and cons, information technology stakeholders are facing a dilemma regarding the extent to which they should allow their technology to be intelligent and autonomous. This dilemma is becoming increasingly salient, as computer algorithms have become ubiquitous with the rise of the Internet of Things (IoT) and mobile computing.

In the proposed research, we focus on the economic value of the autonomy level of computer algorithms that regulate digital platforms. The platforms that we study are essentially intermediaries in two-sided markets, facilitating transactions between two parties: buyers and sellers (e.g., eBay); drivers and riders (e.g., Uber); entrepreneurs and their backers (e.g., Kickstarter); etc. In each domain, some platforms are considered more open than others, i.e. it is easier for a seller to put a product on the market; in those open markets, there are fewer criteria that a product must meet to be included, and the approval process is simpler, and usually faster. For example: the Google Play Store is considered more "open" than the Apple Store. The crowdfunding platform IndieGoGo is considered more "open" than its rival Kickstarter. The "openness" of such platforms is a result of the fact that they enable computer algorithms to screen the offerings submitted to them, sometimes without any human involvement, in contrast to other platforms, which rely mainly on human inspection.

As automated screening processes are more efficient than human-driven ones, they are likely to generate greater numbers of approved submissions (e.g., mobile applications or crowdfunding campaigns). This, in turn, may result in one of two contradictory scenarios: On the one hand, the platform's users

may find the variety of offerings on the automated ("open") platform more attractive than the more limited set of options on the "closed" platform. On the other hand, the greater variety may come at the expense of maintaining the quality of the offerings. Algorithms approve products according to whether they meet some threshold criteria. Unlike a human, an algorithm might overlook defects that are not covered by its predetermined list of criteria, and therefore might approve products that are of low innate quality.

We draw on and add to two streams of literature: First, the work on two-sided markets and peer economy platform and, second, the literature on information flow on digital platforms.

CYBERSECURITY THEORY DEVELOPMENT: THE ISRAELI CASE IN STRATEGIC CONTEXT

LIOR TABANSKY

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? However, public discussions on Israeli cybersecurity are usually detached from strategic context, impeding cybersecurity scholarship and policy efforts. I argue that the common explanations of cybersecurity – e.g. 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. The objectives are:

1. To bridge the knowledge gap by developing an open, fact-based, comprehensive case study of the Israeli cybersecurity policy from the early beginning to date.
2. To utilize the case study to perform a cross-disciplinary analysis of the Israeli cybersecurity in a grand-strategic context; as opposed to information security, legal, military, technical, regulatory and other narratives.
3. To advance a deductive attempt to develop a general analytic framework of national cybersecurity, which provides ample room for non-technical as well as non-military aspects.

I have already collected much of the sources on the evolution of Israeli cybersecurity in previous research. As cybersecurity overlaps national security, one expects the application of the rich Security Studies scholarship to cybersecurity. However, to the best of our knowledge such a cross-disciplinary approach has not been attempted in the Israeli case. Similarly, Security Studies scholars have largely neglected the cybersecurity topic in the West. In attempt to bridge this gap I will apply the literature on Israeli Strategy to analyze Israeli cybersecurity policy.

The general argument is that national Grand-Strategy is the under-researched factor impacting cybersecurity strategy and practice. Hypotheses on how have concepts such as qualitative edge, early warning, force multiplier and deterrence on impact Israeli national cybersecurity posture and capability will be formulated more precisely once the case becomes clearer, and subjected to critical tests. The newly applied scholarship from two realms (Israeli Strategy and Security Studies) in this case study provides for a deductive attempt to develop a general theory of national cybersecurity, which provides ample room for non-technical aspects. Theory building from case studies is an increasingly popular and relevant research strategy that forms the basis of influential studies. This qualitative research method enables us to capture the complexity of the object of study. This research case selection is driven by the global high regard of the Israeli cybersecurity. The findings of the case study enable us to uncover drivers, dynamics, stakeholders, conflicts and hurdles in the Israeli cybersecurity policy for further examination of their relative significance towards a new Cybersecurity Theory with enhanced explanatory power.

This research provides cybersecurity debate with the missing context by utilizing knowledge obtained from the Security Studies literature on National Grand-Strategy to analyze cybersecurity. It presents a theoretical-methodological innovation, with a broad generalization potential. Scholars of

International Relations, Security Studies, Comparative Strategy, Public Policy, Business Management, Organizational Change, as well as policy circles – will find value in the solid factual foundation of theory building and comparative research provided by this case study of Israeli cybersecurity.

DETECTION OF CYBER ATTACKS IN INDUSTRIAL CONTROL SYSTEMS BY INTRINSIC SENSOR DATA ANALYSIS

AMIR GLOBERSON, MATAN GAVISH (HUJI), RONEN TALMON (TECHNION)

Recent years have seen an explosive increase in cyber attacks against industrial control systems (ICS). An additional threat that has received much attention as a result of the recent Stuxnet attack on Iranian nuclear facilities is sensor hijacking. Not only can cyber attackers attempt to gain control over the industrial system, they can also feed false information into the system's sensors, creating a false impression of nominal system behavior at the control room, and keeping the ongoing attack covert while doing harm.

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. The detection systems we propose to develop are stand-alone systems that continuously monitor the ICS without interrupting its function. This proposal describes a significant effort in cyber security of ICS, bringing together theory, algorithms and engineering. Specifically, the proposed project brings together fundamental mathematical research in manifold learning and in control theory, fundamental statistical research in high dimensional sensor data analysis, fundamental research in machine learning under adversarial setting, development of practical and efficient algorithms that implement our fundamental results, and software engineering for implementing these algorithms efficiently.

Objective 1 – **Fundamentals**

- High-dimensional covariance estimation
- Intrinsic state estimation with auto-encoders
- Adversarial Detection
- Optimal control

Objective 2 – **Takeover Detection by Intrinsic State Monitoring**

Objective 3 – **Sensor Hijacking Detection**

Objective 4 – **ICS-TDS Proof-of-concept and Data Collection**

A key component of our proposal is construction of a "toy ICS", such as a software-controlled power generator, fitted with numerous sensors. This system will allow actual proof-of-concept in the controlled environment of a university lab.

We expect to have visible impact on a number of fields in and around cyber security of ICS; to attract academic interest to a variety of fascinating theoretical questions implied by monitoring of dynamical systems in the presence of adversarial inputs and machine learning in adversarial conditions; and to prove that a low-budget experimental system can drive academic research with a revolutionary short turnover time from theoretical ideas to proof-of-concept implementations.

THE DENIABILITY MECHANISM IN THE CYBER AGE - ITS EFFECT ON STATES' BEHAVIOR IN THE INTERNATIONAL SYSTEM

GIL BARAM

One of the unique characteristics of cyber attacks is that it is almost impossible to identify the source of the attack and who was behind it: The Attribution Problem. On the other hand, there have been cases when the attacking state was identified and the attack was attributed to it but it denied its involvement and rejected these accusations. This deniability mechanism is the core of this proposed research.

International Relations has not yet examined the deniability mechanism in this respect. The general literature about deniability was focused on the legal aspects and on questions of responsibility and accountability, and was largely drawn from the field of intelligence studies. Most of that research focused on the options for leaders, mostly in democratic states, to deny their knowledge about certain covert operations carried out in foreign lands during their tenure.

The study will examine the importance of the deniability mechanism in several respects: What is the deniability mechanism; What is its significance in conventional military operations and what are the differences in a cyber attack; What are the factors that lead states to deny some offensive cyber operations but not others; How does the use of the deniability mechanism affects the degree of aggression of states in the international arena.

The underlying assumption of the study is that offensive cyber capabilities allow states greater freedom than before and make it easier for them to use their power in the international arena. The origin of this freedom lies primarily in the possibility of conducting offensive cyber attacks while successfully denying responsibility.

Why would a state choose to use the strategy of denial? Two possible explanations for this question are offered in this study: first, the state denies the attack to avoid a reaction by the international community. This explanation is based on the foundations of the realist paradigm in international relations that emphasizes the importance of power in the anarchic international system.

The second explanation is based on the Audience Costs theory, calming a state will choose to deny the attack in order to make the victim less motivated to respond, reducing domestic pressures on him to retaliate forcefully, and providing the victim more leeway to choose its response, thus also possibly preventing a dangerous escalation.

The study will use the database of Valeriano & Maness (2014) showing cyber attacks between rivals in the years 2001-2011. New relevant data from the years 2012-2015 will be added to this dataset. The study will combine several techniques and methodologies - quantitative and qualitative. First, the *deniability mechanism* will be evaluated in the cyber context and in the conventional context; Second, a statistical analysis will be made of the factors that may motivate a state to deny its offensive cyber activity to create an applicable model that will allow an evaluation of the reasons states chose to deny their actions and how the attacked state should react. Following this, different types of qualitative tests using the Process Tracing technique will be employed to strengthen the reliability of the results obtained in the previous section, with the aim to present insights and conclusions that could be implemented by decision-makers.

The ultimate purpose of this kind of 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

ELI AMIR, SHAI LEVI

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. Our main hypothesis – firms will withhold information on the more severe cyber-attacks and voluntarily disclose the milder ones 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.

THE EFFECT OF ENGAGEMENT ON PRIVATE INFORMATION

NAAMA TZUR, LIOR ZALMANSON, GAL OESTREICHER-SINGER

In this research, we are interested in the dynamic of information disclosure on social media websites. Why do users provide personal information on some website and not on others? What builds up trust at the initial meeting point between a potential user and a website or an application? How does online engagement influence this dynamic?

In accordance with Information Boundary Theory, we propose to examine a trust building dynamics as the following hypotheses outlines:

- **H1:** Website initiated participation influences individual's perceptions of the website.
- **H2:** Individual's perceptions of a website influences individual's information disclosure.
- **H3:** Website initiated participation influences individual's information disclosure.

Our methodology is a random assignment experiment. Using an online website ("VideoBook") that was designed for and described in Zalmanson & Oestreicher-Singer (2014), we propose to examine these three main hypotheses. Through a series of experiment, we aim to isolate and better understand the impact of online engagement on information disclosure.

Participants are recruited mostly via Amazon's "Mechanical Turk". We ask each of the participants to browse VideoBook while presenting her with pop up notifications that vary in type and amount. At the end of the session the participants are requested to answer a questionnaire and provide personal information. We are able to compare the activity log of different participant and the associated answers and information disclosure level. This enables us to analyze the relation between online behavior and personal perceptions.

So far, we have examined the impact of online engagement on trust, privacy concerns and willingness to disclose information. We have found significant differences in the behavior of individuals who were presented with pop up notification in comparison to those who weren't in terms of trust and information disclosure, while no significant change has been detected regarding general privacy concerns. Our contribution to the relevant information system privacy research mainly evolves around the relation between online engagement and information privacy.

ECONOMIC UTILIZATION OF WORKFORCE-BASED LABELING FOR SECURITY APPLICATIONS

TOMER GEVA, MAYTAL SAAR-TSECHANSKY (U. TEXAS AUSTIN)

Supervised learning is a key technology for handling security threats by capturing patterns in historical data that are characteristic of threats, and then detecting these patterns in the future. Supervised learning has been successfully applied to a myriad of important security applications including inappropriate content filtering, intrusion detection, video-surveillance-based intention detection, internet bullying detection, and online fraud detection, among other tasks. Recently, online marketplaces for human intelligence tasks, such as Amazon's Mechanical Turk, have presented exciting opportunities for using human intelligence to enhance or complement data-driven learning algorithms. However, achieving these benefits is non-trivial. For this promise to materialize, it is imperative to characterize and address a myriad of new challenges presented by these marketplaces.

This research aims to be the first to provide a comprehensive information acquisition policy for human labeling markets towards security modeling tasks. As such, it aims to produce a novel labeling acquisition to maximize modeling performance for a given budget and time constraints. To accommodate human labeling markets the policies we aim to develop will also consider the labeling task assignment, the capacity to acquire multiple labels for a single data instance, the pay offered per label, as well as effective incentives and labeler screening mechanisms. Towards that we first aim to develop a novel framework that accommodates the rich set of components of this problem. We also aim to programmatically implement the proposed solution and empirically evaluate its performance in real-world settings over different kinds of human intelligence marketplaces and settings. Empirical evaluations will involve both simulation and live experiments, deploying online platforms for both non-expert and expert workers. The suggested framework includes the development of several modules to address the challenges above. Specifically, the modules include:

A. Continuous evaluation of a labeler/worker quality. This module will estimate the expected tradeoffs function for payment/quality and for payment/time.
B. A data-driven learning module responsible for continuous re-training of supervised learning algorithms.
C. Performance evaluation model - evaluating performance over an independent test set.
D. A "policy" for selecting informative training instances for labeling that would be used for model learning, and the assignment of pay offered per labeled instance. This module will also decide whether there is a need for multiple labeling per instance, and whether or not to invoke screening questions to screen potential labelers. This module will interact with modules (a)-(c).
E. A real-time front end web interface to interact with the online workers and allocate the relevant data instances for labeling.

We expect that this research agenda would yield several research contributions. Specifically, the expected contributions include opening the data-acquisition bottleneck in machine learning security applications, and algorithmic research towards maximizing security performance under budget and time constraints.

EVOLVING CYBER-THREATS AND COUNTERMEASURES: MATHEMATICAL, BEHAVIORAL AND LEGAL PERSPECTIVES

JOACHIM MEYER, RONEN AVRAHAM

The proposed research addresses a set of interrelated research questions, combining analytical (optimization), behavioral (experimental economic and psychology) and legal perspectives. From a behavioral modeling perspective, we will develop quantitative models to predict users' behavior in environments with changing threats and information about threats, and we will validate the models with empirical studies. Under what conditions will end-users be particularly vulnerable to attacks? What will affect end-user's motivation to prevent security threats? We will then extend this research, 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. We will address these questions 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, we 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.

The proposed interdisciplinary research consists of six tightly connected parts:

1) The development of quantitative models of end-user responses to information in an environment where the characteristics of threats, the available information and the value of the information for detecting threats change relatively quickly.
2) An empirical research program, conducted in the laboratory and with actual websites to study responses to different types of information and end-users' ability to determine whether a threat exists at a given moment.
3) A survey of the existing threats and of the emergence of threats, based on the collection over time of threats in phishing messages, malicious websites or content, etc.
4) A quantitative and empirical evaluation (using laboratory and web experiments) of the impact of different alerting messages and policies on end-users responses.
5) The legal part has two main components.
   i) Developing a framework for providing information and responding to changing threats: What is the optimal warning? When is a warning insufficient? Insights will be drawn from the literature on consumers' product liability.
   ii) Developing a framework for incentivizing end-users to take optimal precautions. The legal system is comprised of various legal regimes ranging from full immunity, through various insurance-based mechanisms, to regimes where victims bear at least some costs (Avraham, 2011). The different aspects of the legal framework will be integrated into the mathematical and behavioral modeling.
6) In the last phase of the project we evaluate the optimal design at a system level, given the results from the different mathematical, behavioral and legal analyses.
7) The outcome of this combined, multidisciplinary research can be used to develop interfaces, systems, user education programs, regulations and policies that will jointly lower the negative consequences of cyberattacks.

EXTRACTING SIGNATURES AND FILTERS FOR ZERO-DAY SOPHISTICATED DNS AND OTHER DDOS ATTACKS

YEHUDA AFEK, ANAT BREMLER-BARR, EDITH COHEN (IDC HERZLIYA)

Distributed Denial of Service (DDoS) attacks keep being the number one worry of many infrastructure providers as well as of different enterprises. Usually not only the targeted victim suffers, but there is collateral damage and the neighboring servers and customers suffer from these attacks. In 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. The proposal will entail the development of new algorithms for the analysis of high throughput streaming data (aka 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).

Recently the attackers have developed code (zombie agents) that go under the radar screen of existing defenses, thus evading the mitigation. In the past ten years, these new attack methods included huge (~1 million) zombie armies of agents, each making seemingly legitimate, non-spoofed html (or other such as smtp and DNS) requests. Each of the agents makes the requests at a very low rate (say one every two minutes), however combined from all the zombie agents together it is a large volumetric attack that knocks down the victim servers. To overcome these attacks the first two PIs with their students (Shir Landau-Feibish, and others) have developed a tool that extracts a signature (string of characters) for these attacks within a minute or two from the attack detection. These signatures are then applied at the mitigation device and stop the attack. The premise is that most if not all the agents in the zombie army use the same code, and the code leaves some characteristic finger print on which the mitigation can be based. This has proven to be correct in the mitigation and study of several attacks on actual customers of a local vendor. This vendor has recently successfully used our tool to generate signatures with which it has mitigated the attacks.

That previous work has resulted in the development of new heavy hitters algorithms tuned to the efficient extraction of varying length signatures. However, in the last two years new DDoS attacks have appeared, specifically DNS reflection attacks and DNS amplification attacks. These attacks require the adaptation and extension of our basic tool to deal with these new attacks. Moreover, some of the new DNS attacks and others, use randomization to fool signature extraction based techniques. Basically, by issuing millions of DNS requests, each with a slightly different variant using a short randomized string. From discussions we had with ISPs and local network operators, these attacks are causing major problems, even though often the providers or their clients are not the end target of the attack, but a secondary unintentional victim.

Motivated by a particular randomized DNS attack we will develop new and efficient distinct heavy hitters algorithms and build a system to identify these attacks using the new techniques. Heavy hitter detection in streams is a fundamental problem with many applications, which include detecting certain DDoS attacks and anomalies. A (classic) heavy hitter (HH) in a stream of elements is a key which appears in many elements. When stream elements consist of {key, subkey} pairs, a distinct heavy hitter is a key that is paired with a large number of different subkeys and a combined heavy hitter is a key with a large combination of distinct and classic weights. Classic heavy hitters detection algorithms date back to a seminal work of Misra and Gries (1982) which achieves an optimal tradeoff of structure size to detection quality. We will develop new algorithms for distinct and combined HH detection which will improve on previous designs in both the asymptotic (theoretical) sense and practicality and nearly match the performance tradeoffs of the best algorithms for classic HH detection. Our approach will be based on a novel combination of Sample and Hold weighted sampling and state of the art approximate distinct counters. Finally, we will design a system for detecting randomized attacks on the Domain Name System (DNS) service, which will be based on our distinct and combined HH detection algorithms, and demonstrate its effectiveness through an experimental evaluation on both real and synthetic attacks.

GUIDING AND INCENTIVIZING CYBER-SECURITY BEHAVIOR

ERAN TOCH

Humans are consistently referred to as the weakest link in cyber-security. While cyber-security technologies provide a powerful technical solution, employees' failure to comply with enterprise security guidelines is the cause of the majority of breaches in enterprise computing. Mounting evidence prevents us from anymore assuming that users will simply follow the organizational cyber-security policy. To create an effective security environment, we need to understand and develop systems that would incentivize users to adopt positive cyber behavior.

Recent studies are focused modeling user reactions to cybersecurity systems, showing that disciplinary action has only marginal effect in making employees comply with cyber-security systems [1,3], and that by adapting the cyber-security response to users, we can increase the overall security [5]. However, established theories of human cyber-security behavior, such as Protection Motivation Theory (PMT) and the Theory of Planned Behavior, take for granted that users must use the system, and thus do not take into account the need to incentivize the user to use the system and to comply with its policies [5]. We turn to the literature of behavioral economics and human-computer interaction as an inspiration for finding ways to incentivize and guide users. One major concept we turn to is **gamification**, defined as applying game and design techniques to non-game applications to engage users. However, to the best of our knowledge, there is still no understanding on how gamification can be used in the context of the cyber-security system's interaction with users, and how can non-monetary methods can be used to influence and guide users' behavior.

We suggest to conduct 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; **second**, to test how can we influence users' decision-making processes by designing gamification-based incentive systems. By the end of the study, we plan to offer a toolkit for optimal design of incentive systems for cyber-security that enhance the user involvement in the interaction in enterprise security systems. Our working hypothesis is that a successful system of incentives can balance the negative incentives by adding explicit gamification incentives. Given that most cyber-security risks are abstract, adding explicit incentives can make a significant and measurable change in users' behavior. We will test the effects of incentive systems in comparison to standard blocking and warning techniques, how different types of incentives fare (e.g., scoring versus leaderboards), and what are the effects of negative incentives versus positive incentives.

The research will combine theoretical and empirical aspects, taking specific types of enterprise cyber-security scenarios as the basis for a series of experiments with human subjects that aim to evaluate our theory. The research methodology will involve: (1) Reviewing the current and the relevant behavioral economics and human-computer interaction models; (2) developing models of human decision-making that reflect a cost/profit behavioral economic model with the possibility of evading the system; (3) empirically evaluating these models using data from real-world cyber-security systems; (4) designing incentive systems for influencing users towards particular outcome; (5) conducting controlled experiments with human subjects to evaluate decision-making processes and the effects of incentive systems.

The empirical real-world analysis will be based on data that was provided by Checkpoint Inc., which describes how users in a large enterprise interact with UserCheck, an application that alerts users of suspected breaches and allows the user to authorize of legitimate communications. Our initial analysis of the data provides a promising start to model the users' interaction with the system. The controlled experiments will be based on "Security-Robot", a technology developed in our lab, which is used to recreate cyber-security experience for users. It can be used for simulating systems such as malware detection and URL filtering using a Chrome browser extension. We plan to measure the user's behavior with well-established measures from the domain of usable security, including behavioral modeling, perceptual impact of security feedback (using eye movement analysis and other means), and user satisfaction measures.

INFRASTRUCTURE FOR CYBER THREAT INFORMATION SHARING

TOVA MILO, DANIEL DEUTCH

Upon detecting Cybersecurity threats and vulnerabilities, security analysts refine their security policies so that similar events may be avoided in the future. However, threats are often identified only when serious damage is already done. Sharing the technical data on that threat, vulnerability, as well as the means to identify and/or overcome it, can help others account for the threat or remedy the vulnerability before it is exploited. This is referred to as cyber threat information sharing. This project focuses on development of the enabling Information Management technology to support such cyber threat information sharing, which in turn is expected to improve the effectiveness of defensive cyber operations and incident response activities.

Research Questions and Challenges

Large-scale Data Integration. A core issue here is that of combining and integrating information from multiple sources. This information includes logs related to the event, ways in which it was identified and addressed, as well as relevant meta-data (see below). A significant difficulty in Data Integration is that each organization (and each system) uses different schema, format and terminology to describe the same type of knowledge. Dealing with data that is large-scale and distributed across multiple peers and applications poses further difficulties in the integration process.

Handling Meta-data. Beyond pure data (such as logs and alerts), to allow for effective use of the data, applications should share meta-data of various domains, such as rules or inference processes and workflows, derived (classification) rules, user insights on the data etc. Meta-data modeling, management, analysis and sharing should all be addressed in this novel and complex setting.

Integration while preserving Privacy. While information regarding actual threats should be shared, it is essential to avoid as much as possible compromising the privacy of "innocent" users and organizations. A difficulty is that there may be intricate connections between the different components. Incorporating Human Input. the process will be partially assisted by input from experts, validating identified threats and/or rules and supporting integration. Naturally experts input is a costly resource, and so an important research goal is to optimize the tradeoff between requiring minimal such input and obtaining results of good quality.

2 Expected Outcome

Model. A first expected contribution is a unified model for cyber threat information sharing, one that can also serve as the basis for the information analysis, and ultimately lead to a more effective treatment of such threats. In particular, data that should be modeled (and then shared) includes the following components: (1) logs of events that were captured and identified (or suspected) as cyber attacks; (2) for each event, meta-data that is associated with it, such as participating entities, status of the system at the time etc; (3) logic underlying the reasoning that is applied to identify threats. The logic should be shared even in absence of events, and furthermore when events are shared, the particular part of this logic responsible for its discovery should be identified; (4) actions that have been done to address threats, again in correlation with the logged events.

Algorithms. We then expect to develop efficient algorithms that support integration and sharing of cyber threat information while accounting for privacy and meta-data, as well as for the unique features required here, including timeliness, possible errors and contradictions in the data, and its heterogeneity. Since it is expected that cyber threat information sharing is not done in a fully automated way, we will develop algorithms that effectively incorporate feedback by domain experts while minimizing their effort. We will further strive to validate our solutions through prototype implementation and experimentation where applicable.

HOSTILE INFLUENCE OPERATIONS VIA SOCIAL MEDIA: A CYBERSECURITY ISSUE? ASSESSING THE APPLICABILITY OF RECENT EVIDENCE TO THE ISRAELI SOFT POWER

LIOR TABANSKY, MARGARITA JAITNER (SWEDISH DEFENCE COLLEGE)

Cyberspace in general and Social Media in particular provide new and affordable tools for actors to pursue their interests. The risk of political debate and decision-making being influenced by hostile Influence Operations is no longer theoretical since 2014. This interdisciplinary research aims to develop a new analytical framework for cyber power, explicitly including defense against hostile against Influence Operations via Social Media. The interdisciplinary research team consists of multilingual junior scholars to utilize original primary sources. The team has expertise in: Cybersecurity policy, doctrine and strategy; Strategic Communication; Social Media.

RQ1: Whether and how has the Western defensive posture regarding Influence Operations changed since 2014? We focus on uncovering and analyzing the recent shift in threat perception that resulted in NATO and EU research and policy efforts to address defense against hostile Influence Operations. The team includes a leading junior scholar of Influence Operations via Social Networking.

RQ2: Can the latest Western research on defense against hostile Influence Operations via Social Media contribute to the Israeli societal resilience and Soft Power? We study whether and how two Open Societies – Finland and Israel – perceive societal resilience in these two countries. The team includes a leading junior scholar of Israeli cybersecurity.

RQ3: How could the realms of defense against hostile Influence Operations via Social Media and National Cybersecurity overlap?

We expect to demonstrate positive answers to RQ1 and RQ2. We develop an integrative framework between traditional cybersecurity efforts with countering hostile Influence Operations to increase societal resilience and Soft Power.

IDENTIFICATION OF MALICIOUS WEBSITES BY LEARNING THE WEBSITES' DESIGN ATTRIBUTES

IRAD BEN-GAL, DORON COHEN

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.

This research will use machine learning techniques to identify malicious websites, while utilizing advanced feature extractions techniques on HTML design features. The proposed solution will enable:

1. To increase the sample size by automatically analyze thousands of websites in a minute while improving the algorithm run-time for massive load. At this point the beta version of the algorithm analyzes semi-automatically only dozens of websites in several minutes. Increasing sample size will also yield more interesting patterns and features for identifying not only crack websites but also other website categories.

2. To increase the number of analyzed features t this will allow us to better understand complex patterns and improve the identification rate.
3. To add more machine learning procedures and algorithms for a dynamic "Learning and improve" process that can be further used as a black box kit.

Preliminary Results

We built a classification model using different random-forest configurations with 10-folds cross-validation learning, classify and test them on "Google's top 1000 sites" category. Based on initial search results we were able to isolate and add a small "black list" of crack websites to the supervised learning process. For each website, we calculated ~1100 design attributes, such as: element type (tag name); element color and tone; text font size (in pixel); text total rate; text color length and many more features. We also learned various relations among the calculated features (normalization, averages, covariance, ratios etc). We show that the classification by both key words and HTML design features (without using computationally-extensive text-mining procedures) can be used to identify malicious websites in a tractable manner. In particular, we show that using the website design features in addition to simple meta-keywords, can significantly enhance the predictability of malicious websites up to a high accuracy level of ~97.8%.

THE INTERPLAY OF CYBER VULNERABILITY AND ENTERPRISE CREDIT RISK

SHACHAR REICHMAN, SAM RANSBOTHAM (BOSTON COLLEGE), GEORGE WESTERMAN (MIT)

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.

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. Specifically, we will focus on the following hypotheses:

1. An increased cyber vulnerability of a firm increases the probability of the firm's credit rating downgrade.
2. A credit rating downgrade of a firm increases its cyber vulnerability.

Taken together, the two hypotheses predict a circular relationship between cyber vulnerability and credit downgrade. To study this relationship, we will first 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. This potential endogeneity requires careful econometric identification, an important component of our proposed research.

First, we introduce a conceptual framework that illustrates the mutual effects of cyber threat and credit downgrade, accounting for other mediating factors. In the empirical part of the research, we plan to study and quantify the effect of each of the variables in the framework on the financial and security risk of a firm. Following the research hypotheses, we focus on two key aspects of this framework: (1) how cyber vulnerability may affect a firm's financial performance and influence operational stability of a firm, and (2) how a credit rating of a firm, specifically a downgrade, affects cyber vulnerability. The second part of the framework deals with the outcome of a firm's credit

downgrade, describing the consequential events and activities and how they may lead to an increased cyber vulnerability.
We will empirically investigate the proposed model by analyzing security, credit, and related events for the Fortune 500 companies. We plan to develop models to estimate the effects described in the conceptual model:

1) How does security vulnerability directly affect credit rating?
2) How does credit rating downgrade affect a firm's security vulnerability?
   a) How does credit rating downgrade affect internet presence and the subsequent security risks?
   b) How does credit rating downgrade affect firm financial activities and cyber security activities?

We will use machine learning algorithms to empirically analyze these data in order to generate a quantitative longitudinal approach that relates cyber vulnerabilities and incidents to the financial stability of firms.

THE INTERSECTION OF CYBERSECURITY AND SPACE SECURITY: NEW THREATS AND THE DEVELOPMENT OF LEGAL AND POLICY RESPONSES

DEBORAH HOUSEN-COURIEL

Cyberspace and outer space may be characterized as interdependent elements of a complex and continually-evolving nexus of activity for state and non-state actors. Thus, many of the current challenges to one domain also pose issues for the other.

Research questions:

- What are the legal norms applicable to the hostile disruption of satellite communications, either by physical harm to the satellite or virtual disturbance to its transmissions?
- Under what circumstances do cyber operations against satellites constitute an illegitimate use of force, thus permitting a state to engage in self-defense under the collective security regime?
- To what extent do present international law norms in fact provide a relevant and effective paradigm, including enforcement and remedies, for coping with these scenarios?
- How are the international legal and policy communities engaging with these challenges at present?

This research will analyze the international legal and policy communities' present encounter with the vulnerabilities of national and commercial activities in cyberspace and outer space. Efforts such as those under the aegis of the UN's Office for Outer Space Affairs, its Office for Disarmament Affairs and its First and Fourth Committees; the European Union, the Council of Europe, the Organization for Security and Cooperation in Europe, NATO and the Shanghai Cooperation Organization have addressed a number of issues that have ramifications in both the cybersecurity and space security context. Specifically, the research will analyze the reports of two separate Government Group of Experts (GGE): the 2013 Report of the GGE on Transparency and Confidence-Building Measures in Outer Space Activities ("the Space GGE") and the 2015 Report of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security ("the Cybersecurity GGE"). At present, these efforts are "siloed" and do not interrelate at either the normative or enforcement levels.
The research will propose a model for moving forward to reduce the vulnerabilities of satellites and satellite communications through a more focused and coordinated process of legal - normative clarification and enforcement mechanisms in both contexts.

A MACHINE LEARNING COLLABORATIVE STUDY OF LANGUAGE-ACTION CUES FOR SPONTANEOUS DECEPTIVE COMMUNICATION AND CYBER-ONTOLOGY DEVELOPMENT

ODED MAIMON, SHUYUAN MARY HO (FLORIDA STATE UNIVERSITY)

In this study, we will examine the use of deceptive language, and explore language usage patterns during online deceptive acts. As interpersonal communication is defined as a dynamic exchange of messages between or among two or more people, our research will focus on social interactions where participants try to mutually influence each other in a dynamic fashion. We thus seek 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?**

Methodology: Online Game

For this research, we plan to focus on developing specific metrics for language usage patterns and information behaviors. We will set up online game scenarios to analyze communication dynamics that distinguish between different types of communication typologies for further investigation into the underlying patterns and their relationships to words used. To mimic various deceptive scenarios, an interactive online game has been designed for collecting data on the dynamics between two actors as they are presented with choices to deceive – or to detect deception.

Data on participants' truthful (as baseline) and deceptive statements, as well as their interpretations will be collected and stored in a database. New machine learning techniques will be applied to proceed from previous experiments that proved feasibility, to state of the art tools. The promising results were obtained using Linguistic Inquiry and Word Count analysis; and regression analysis to estimate the relationship between predictor variables. The next stages include text mining, and new cyber-ontology development.

Results of Prior Study

The best result for the dataset of our prior study was R^2=0.967, p=0.03. This study suggests promising results for modeling deceptive language cues. Games like this can be further employed to collect a large, synchronous dataset. Future research includes improving the design of the game to minimize the effects of dynamic factors, validating deceptive and trustworthy cues, and broadening the framework to a solid cyber-ontology of deceptive language.

NETWORK ATTACK AND DETECTION IN MODBUS/TCP SCADA SYSTEMS

AVISHAI WOOL, LEONID LEV (ISRAEL ELECTRIC COMPANY)

SCADA networks for Industrial Control Systems (ICS), which rely on commercial off the shelf (COTS) communication equipment, are vulnerable to various attacks. In prior work, Prof. Wool and his students have suggested an extremely efficient model-based anomaly detection system for such networks. The system automatically constructs a sensitive semantic model based on a deep inspection of the traffic, yet the model's enforcement can work in real time, at line speed, since it only relies on deterministic finite automata (DFA) at enforcement time. The approach was demonstrated to have extremely low false-positive rates over benign traffic recorded on the production system monitoring electricity usage in the TAU campus. However, evaluating the approach's ability to detect true attacks is still open, primarily since it is very challenging to obtain access to a realistic ICS against-which one could launch attacks. Furthermore, we would like to evaluate the approach's success on other ICSs. The goal of this research project is to address these open questions. A key ingredient to the success of the project is the availability of the Hybrid Environment for Development and Validation (HEDVa) lab at the Israel Electric Company, managed by Dr. Lev. The HEDVa lab has been used in EU FP7 research projects and includes electrical and telecom equipment, virtual machine infrastructure, test-environment network-flow management infrastructure, a SCADA management system, an Electrical infrastructure

simulator, and additional support components. The SCADA system implemented in HEDVa uses the Modbus/TCP protocol.
Another aspect of the project is a collaboration with the lab of Prof. Frank Kargl at U. Twente in the Netherlands. Prof. Kargl has access to Modbus/TCP traces recorded on production ICS systems of Dutch utilities, and is happy to collaborate with us. However, since the Dutch data is considered sensitive, and is owned by the utility companies, it must remain at U. Twente. Therefore, to evaluate our anomaly-detection system on this data, we need to perform the experiments on site in Twente.

Research plan

1. Developing network penetration-test tools specifically for the Modbus SCADA protocol. We plan to develop a suite of tools that can mount network-based attacks with variable levels of intrusiveness and stealth: from passive network monitoring to active connection attempts, with or without IP spoofing, targeting either the PLCs (equipment controllers) or the HMI (operator console). Our stealthiest attacks will involve TCP hijacking, placing the penetration-test device as a man-in-the-middle. In all penetration scenarios we plan to inject Modbus-level commands, either to take control of a PLC and/or to feed the HMI with fake data, or both. This task will be implemented by an M.Sc. student, under the supervision of Ph.D. candidate Amit Kleinmann.
2. Experimentation with the penetration tools: We plan to deploy the penetration-testing tools on the IEC HEDVa environment and evaluate their abilities, without deploying any counter-measures. This work will be done by a 2nd M.Sc. student, with significant support by several IEC staff members, with expertise in Networking, Server administration, and Industrial Control.
3. Testing the model-based anomaly-detection system on data from the IEC HEDVa environment and from U.Twente. We have already received some data traces from both environments (of benign traffic, without any attacks). Preliminary analysis by Amit indicates that the traffic is generally very well modeled by our system. However, we did observe some phenomena that did not manifest themselves in the TAU electricity monitoring system. We plan to generalize our system to allow modeling the benign traffic observed at both environments, with a minimal amount of false alarms. Analysis of the data from U.Twente will require Amit to travel to the Netherlands twice a year, and spend 2 weeks at Twente in every trip.
4. Testing the anomaly-detection system against the penetration tools: we plan repeat the experiments of step (2) in the HEDVa environment, and evaluate how well the anomaly-detection system (after the improvements of step (3)) can detect the attacks. This will require the involvement of all the TAU team members, supported by the IEC team.

MITIGATING THE RISK OF ADVANCED CYBER-ATTACKERS

OHAD BARZILAY, ASHER TISHLER (COLLEGE OF MANAGEMENT), AMITAI GILAD

This study develops defense strategies against sophisticated and well-funded cyber-attacks (such as **Advanced Persistent Threats, APT)** that can cause extensive damage to major organizations. We develop and analyze a game between a cyber-attacker and a defender operating a network that manages a large organization (such as a bank or an electric utility) in which the defender moves first and deploys blocking and/or detection measures to protect her network from cyber-attacks. Then, the attacker, who has learned the network structure and defense profile, attempts to deliver the maximal

flow of malicious elements to a target node, possibly by investing in R&D to avoid detection and bypass blocks.

We pose the following research questions:

1. How should the risk of advanced cyber-attacks be incorporated into the defenders' decision-making process?
2. Whether and how do optimal defense strategies against advanced cyber-attacks differ from common practices?
3. How intrinsic considerations, such as the characteristics of various cyber-technologies and the network structure, affect the attackers' R&D processes and operational efforts?
4. Is it advantageous for several organizations, which may or may not be competitors in the same marketplace, to cooperate in defending against advanced cyber-attacks?

We expect the following major contributions:

1. To define and analyze advanced cyber-attackers' strategic decision-making by incorporating the attacker's desired volume of malicious flow and R&D investment, as well as the intrinsic characteristics of defense measures, the players' budgets and costs. Our models will account for the attacker's strategy and reaction to various defenders' strategies.
2. To propose an organizational defense approach for allocating resources to cyber-defense technologies in networks, in an attempt to mitigate the risk of advanced cyber-attacks.
3. We expect to advance the body of knowledge regarding the value of defenders' deterrence and deceit efforts, which is a growing trend in mitigating such risks in practice.
4. We expect to shed some light on regulatory measures in a country's defense against **APT**.

NON-PUBLIC FINANCIAL INFORMATION LEAK

ROY ZUCKERMAN

The exploratory study of the role of cyber security in non-public information leaks will examine whether firms properly oversee the online security measures takes to protect non-public financial information both within the organization and with the affiliated service providers. In addition, we will attempt to identify certain service providers which are more likely to be associated with leaks and determine if those are associated with weak cyber security measures.
Recent scandals have demonstrated the preponderance of trading based on insider information in financial markets. In one of the more prominent insider trading scandals, Raj Rajaratnam of Galleon Group, was recently convicted of a series of illegal trades based on a network of non-public information he received from company insiders, among them Rajat Gupta, the former head of McKinsey & Company, who served as a director on the board of Goldman Sachs. Another major case has involved the large hedge fund SAC Capital, where traders have used complex networks to relay non-public information from corporate insiders to fund equity traders. These leaks involved some of largest traded technology firms, including Dell and Nvidia, and resulted in hundreds of millions of illicit gains. These examples involve leaks from company insiders, however, many of the cases prosecuted by the SEC involve leaks, not only from company insiders, but also from third parties who are exposed to the non-public information, such as accountants, lawyers, and even PR firms and Financial Printers. So far, the focus has been on human-to-human information transfer, but this must not necessarily always be the case. While human-to-human leaks of non-public information poses a challenge to law-enforcement, a far bigger challenge may be posed by leaks generated from cyber space. In October 2012, R.R. Donnelley and Sons Co., a "Financial Printer" accidently leaked Google's earnings report hours before the scheduled release by filling an online draft of the release with EDGAR. Concurrently, The sophisticated data theft from Target Corp. demonstrates the potential for leaks of material information through cyber hacks. While the primary objective in the Target hack was apparently customer and credit card information, it

is more than conceivable that other non-public information was retrieved, including non-public financial information, which could potentially be used for illegal trading activity.

Pareek and Zuckerman (2014) have found in a recent study that large price moves during the final 30 minutes of trading, prior to a scheduled after-hours earnings announcement, predict the direction of the earnings surprise (SUE) and post-announcement returns. However, the result does not hold for longer time frames (3 hours and beyond), suggesting that the information is obtained only a short-time prior to the scheduled release. Brenner et al. (2014) have found a similar result in options trading prior to merger announcements. Pareek and Zuckerman (2014) also find that some firms tend to be "repeat offenders" and are more likely to have consecutive leaks.

Despite the circumstantial evidence suggesting that material non-public information may be leaked through cyberspace, little to no research has been done to try to identify the sources of these leaks and to examine whether the security measures taken by firms and affiliated entities (accounting, legal, printing, PR, etc.) are appropriate in preventing such leaks. Unlike hacks designed to obtain credit card or other personal financial information, hacks designed to obtain non-public corporate information may cause just as much damage, but are less visible due to the nature of information obtained. Moreover, firms may have far less incentive to disclose such hacks.

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 finding of such a study may be far-reaching.

NOVEL METHOD FOR INSIDER THREAT DETECTION

INA WEINER

While cyberattacks are typically connected with outsiders' attacks, it is becoming increasingly recognized that an equally great threat to an organization's security lies within. Traditional IT security tools are ineffective for insider threats because they are designed to protect the perimeter, primarily stopping attackers from gaining access. More recently, big data analytics, and behavioral analytics in particular, has become an essential tool for security monitoring. However, what is overlooked is that most malicious insiders do not exhibit suspicious activities. Rather, "insider misuse occurs within the boundaries of trust necessary to perform normal duties."

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. Pupil size is under the control of the autonomic nervous system (along with other involuntary functions such as heart rate and perspiration), which by constricting or dilating the pupil's diameter, regulates the amount of light entering the eye. The sympathetic branch, known for triggering "fight or flight" responses when the body is under stress, induces pupil dilation, whereas the parasympathetic branch, known for "rest and digest" functions, causes constriction. But pupils respond not only to light. Hundreds of psychological experiments have shown that pupil dilation accompanies arousal, cognitive effort and load, attention, recruitment of executive control, and emotions. **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. Of course, people become aroused, stressed and attentive not only when they perform illicit activities. Therefore, the pupillometry-based alerting system will be activated under two conditions: 1. automatically at random times to obtain and store baseline measurements against which anomalies will be evaluated and 2. when an employee logs in to malicious activity-sensitive target systems defined by the organization. Examination of the logs during the time of alert will enable an immediate decision of whether a malicious activity has been performed.

Windows 10 Hello with Intel Real Sense 3D camera system includes algorithms for user recognition based on fingerprints, facial recognition and iris scanning technologies. If such cameras become standard, they could be programmed for pupillometry.
In summary, 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.

PERSONAL GENOMIC DATA: PRIVACY AND SECURITY ASPECTS

BENNY CHOR, METSADA PASMANIK-CHOR

The proliferation of DNA sequence data poses many threats to personal privacy. In the proposed research, we will explore various facets of this threat. We will focus primarily on multi party tasks that involve a large number of participants, where it is infeasible to communicate among every pair of participants, and some form of mediation is necessary. Our work will span both cryptographic and biological aspects. Specifically, we will investigate the following topics:

- A privacy/communication tradeoff: The moderator model.
- Identifying relatives privately in the moderator model.
- Seeking "uninformative" genomic bio markers.
- DNA as a source of biometric applications.

We plan to develop an appropriate theoretical foundation, as well as implementations up to a concrete prototype, where applicable.
New sequencing technologies generate larger amounts of genomic sequence data at higher speed and decreasing cost. This data deluge opens up exciting opportunities in a variety of fields, e.g. medicine, genetics, plant science, bacteriology, and virology. DNA profiles are used by law enforcement authorities, such as the FBI, to solve crimes and identify missing persons. The flip side of this data deluge is the potential for compromising the privacy of individuals, whose genomic data was extracted, analyzed, and stored. Leakage of such data has profound effects on one's privacy, and may lead to social consequences, such as employment discrimination, and availability and cost of health services and insurance. There are several well known cases where privacy of genomic data was compromised.
We plan to study several aspects of multi party computations, which are based on genomic DNA markers. We propose a specific model, the moderator, which enables a substantial saving in communication, at the cost of partial, restricted privacy leakage. We will study the well-known, concrete problem of finding relatives, explore its relevance to the moderator model, and strive to design solutions that are both communication efficient and, to a large and measurable respect, privacy preserving. Since some bio markers will be revealed to the moderator, we will initiate a study of the relevant genomic database in order to identify non informative bio markers. Finally, we intend to investigate the use of genomic data for biometric applications.

PHOTONIC EMISSION SIDE-CHANNEL CRYPTANALYSIS OF SECURE HARDWARE DEVICES

AVISHAI WOOL

The Photonic Emission Side Channel

Side-channel cryptanalysis has been an active field of research for the last 15 years. Over the last 3 years a new and exciting side-channel been discovered.

Prior work

Work by Prof. Wool's group focused on the power-analysis side-channel and showed how to mount key recovery attacks on a secure device based on careful measurement of the power used by the device during execution of the cryptographic function. Their approach was to represent the cryptosystem, and the leaked side-channel information, as a set of constraints or equations, and then to use a suitable solver to find the key. The solver-based approach has two attractive features that we plan to rely on in the current work: (1) it requires an extremely low amount of measurements; (2) it can overcome noise

by embedding a suitable noise model directly into the equations, without requiring multiple measurements.

Goals of the Research

Our goal in the proposed work is to apply the methods and know-how we developed on the power-analysis side-channel, and apply them to the photonic emission side channel. A solver-based approach allows a much better description of the very detailed information leakage which can be exposed by the photonic side channel. However, in all previous attacks which were employed so far to model the photonic emission side-channel, this very specific information was not considered at all. Current successful attacks rely on statistical methods – which require a large number of measurements. We believe that using a constraint-based description of the emissions we can drastically reduce the amount of data that is needed to mount a successful attack.

Research plan

1. **Constructing a Photonic Model Simulator:** We shall create a software-simulated model of the physics of the photonic emission side channel, and calibrate it using the experimental results obtained by the Berlin team. This will allow the TAU team to quickly experiment with various photonic measurement configurations, without the costs and time required for lab work.
2. **Designing a Cryptographic Solver:** One of our goals is to replace the very large numbers of traces with a custom constraint-based solver. We believe that a photonic trace of the emissions during two AEF rounds includes enough cryptographic constraints to allow reducing the remaining entropy to a very small number, i.e., reducing the number of possible keys down to a handful.
3. **Dealing with Noise:** We plan to use the model simulator as a front-end to the cryptographic solver, via a *decoder* that takes the simulated signal and converts it into discrete values for the solver.

   We plan to evaluate the sensitivity of the combined system to measurement noise, and to embed noise-resilient mechanisms into both the solver and the decoder.

PRIVACY BY DESIGN BY LEGISLATION

MICHAEL BIRNHACK, AVNER LEVIN (RYERSON, CANADA)

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.

How can a cybernetic system achieve the optimal combination of usability, security and privacy?

One answer is to take privacy and security into consideration from the very beginning and throughout the lifecycle of the technology in question. This is the idea of Privacy by Design (PbD). PbD's principles express the viewpoint that security is strengthened by PbD. The PbD approach to cyber-security was described by Ontario's Information and Privacy Commissioner as a 'paradigm shift', from a zero-sum game where security is at the expense of privacy, to a positive-sum situation. For example, taking privacy into account when designing a new system would insist on minimal data collection without limiting functionality ('Full Functionality' principle), which requires that privacy not come at the expense of security or other product features. The 'End-to-End Security' principle requires a design that will ensure the protection of data throughout their entire life-cycle. The notion of **Security by Design** was suggested as the application of PbD to areas such as Enterprise Architecture and Software Security Assurance.

However, it turns out that PbD is easier said than done. We identify one exception, which is when the law interferes and requires a PbD process. Given that at this point, many cyber systems are public or governmental, or are in fields that are typically regulated (such as the financial sector), PbD is especially relevant for cyber systems. Accordingly, we examine cases of **PbD by Legislation**, as opposed to PbD by market players. We study a few cases from Canada and Israel. The goal is to identify the optimal conditions for a successful PbD for cyber systems. In Canada, the Ontario Lottery and Gaming Corporation is implementing facial recognition technology to identify addicted gamblers utilizing biometric encryption as a result of following the PbD approach. In Israel, an example is a 2014 regulation as to the primary elections in political parties. The regulations set the exact manner in which a party can update its own registry of members, using the national registry of the population. The process is to be conducted by the Ministry of Interior, after close inspection of various conditions, and in a way that is meant to assure that data is not leaked, that no excessive data is provided, and that integrity and data security are maintained.

The project's **goal** is to identify the optimal conditions for a successful PbDbL. The **expected results** are a better understanding of PbD, its cyber-security aspects, its challenges, and the conditions in which the 'design approach' may work, as well as identifying new challenges, to the extent we will find such, in the application of PbDbL. The expected conclusions would be relevant in determining the conditions under which the application of PbD to the design of cyber systems in general, and cyber security aspects more specifically, will succeed.

RECONCILING CYBER-SECURITY RESEARCH WITH PRIVACY LAW: THE VIDEO ANALYTICS AND MEDICAL IMAGE ANALYSIS EXAMPLES

NAHUM KIRYATI

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.

The overall objective of this research is to remove obstacles to research in video content analysis, medical image analysis and additional fields that require training and evaluation of data that can only be obtained from privacy-sensitive databases. If successful, the suggested research will open the door to research in academic institutions and small and medium enterprises (SME's) on major topics that have essentially been the exclusive playground of database holders. The vision of this proposal is democratization of research. Leaving the enormous value of big data in the exclusive hands of the arbitrary data holders

is inefficient. Resolving the privacy concerns is the key to tremendous progress in crucial domains, such as health and homeland security. The effect of deep learning and its future developments on artificial intelligence, and on society in general, might eventually be comparable to the computing and networking revolutions. The move from exclusive mainframes to personal computers, and the move from the exclusive Arpanet and Bitnet networks to the Internet, demonstrates the value of democratic, competitive research environments. This proposal aims to promote an analogous move with respect to big data needed for research. Accomplishing this goal requires an interdisciplinary approach, involving technology, law and policy.

Research Plan

1. Revealing the public benefit of research access to big data
2. Quantifying the necessity of big data for deep learning
3. Non-destructive anonymization and distributed deep learning
4. Access to research data: an Hohfeldian perspective
5. Propose regulatory amendments to maximize the extractability of public benefit from privacy-sensitive databases, while providing appropriate privacy protection
6. Develop a binding ethical code for researchers

ROBUST DECENTRALIZED DIGITAL CURRENCY

AMOS FIAT, IFTACH HAITNER, ERAN TROMER, BENNY APPLEBAUM

Bitcoin is the first digital currency to achieve widespread worldwide adoption. This is evident from the market value of these digital coins, totaling (as of today) over 3 billion USD held by users in over 3 million digital wallets, and by the rapid acceptance by merchants, which has now expanded beyond online merchants to stores and hotels. The rapid adoption of Bitcoin is due to a combination of factors. First, Bitcoin is decentralized, with no central party holding control over transactions; some users find this ideologically appealing, but for most users, the main value of decentralization is that payments can be sent across the globe within minutes at negligible cost, avoiding the high fees extracted by centralized "choke points" in conventional currencies, and the associated and burdensome procedures. (Attractively for some users, the decentralization also hampers oversight by states' law enforcement; we discuss this below.). Second, the mechanisms underlying the currency (moto: "in cryptography we trust") are perceived as very robust to attack, manipulation or failure - perhaps more so than some national currencies and banks. Third, the Bitcoin protocol is a very flexible and powerful one, that allows automated applications that were previously possible only through expensive mechanisms like trust funds and legal escrow. And fourth, the Bitcoin protocol financially incentivizes participants to participate in the "mining" computation that facilities the currency's own stability and growth. These are recognized and pursued by a large community of users, developers, investors and advocates.

The current and prospective deployment of Bitcoin, or currencies derived from it, raises important challenges. We propose to study essential aspects in the security, economy and policy implications of Bitcoin-like digital currencies. Via the perspectives of cryptography, distributed computing, computer engineering and algorithmic game theory, we aim to improve understanding, identify flaws, and create new systems that serve society better in functionality and robustness.

Among our research goals are: (1) studying better approaches for securing the distributed ledger; (2) developing new approaches for enforcing privacy, regulation, accountability and policy; and (3) studying other decentralized applications beyond bitcoin. We plan a broad investigation of these issues, bringing to bear our expertise in cryptography, computer engineering and Algorithmic Game Theory. We will pursue 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.

SAFETY AND PRIVACY OF MOBILE APPLICATIONS THROUGH MODEL INFERENCE

SHAHAR MAOZ, ERAN TOCH, ERAN TROMER

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): experts in model inference and experts in cybersecurity.

With respect to providing a platform for trust, we propose a project, which realizes a system named AppMod, with several objectives:

1. Logging detailed app behaviors: Designing and evaluating a method to generate rich fine grained logs capturing app behavior efficiently. Specifically, the method need to track how information flows in an Android app, link related events and their control and data flow dependences, and output them in a succinct log, without sacrificing responsiveness of the app and consuming much energy.
2. Building and analyzing application process models: (a) Designing and evaluating a method that infers an expressive model that captures common behaviors of a mobile app. Specifically, the method generates a model that captures control and data flow constraints, which serve as a signature of an app, from rich fine-grained logs of app events. (b) Designing and evaluating a method that efficiently detects violations of an app signature captured in a model. Specifically, the method scans a fine-grained log capturing an app's behavior (in an online or offline fashion) and checks if it deviates from the model by violating some of its control and data flow constraints.
3. Understanding how users can effectively control their privacy and security in mobile platforms: Designing and evaluating user interaction models that make use of information flow and program modeling to effectively control access to the data and to foster trust relations with the application. Specifically, we will analyze how different interaction models can help users make informed decisions in an effective way. We will also study how different communities of users, such as power users, senior citizens and children, matching interaction techniques to the digital literacy and cognitive abilities of users.

To carry out the project, we plan 3 overlapping Work Packages (WPs) as listed above.

SCALING SYMBOLIC REASONING FOR EXECUTABLE CODE VIA SUMMARIZATION AND INTERACTION

NOAM RINETZKY, MOOLY SAGIV

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 craft an unexpected, yet seemingly benign inputs, that can derail the 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: (i) simplifying the generated logical formulae using sound information obtained from static program analysis, (ii) designing domain-specific theories suitable for reasoning about low-level code, (iii) making the reasoning modular by developing symbolic procedure summaries, and (iv) leveraging high-level guidance from the user to identify promising code parts to explore.

SECURING SERVERS AND ENDPOINTS USING SOFTWARE GUARD EXTENSIONS

SIVAN A. TOLEDO, ERAN TROMER, SHAY GUERON (HAIFA UNIVERSITY)

Cloud computing offers many benefits to organizations, but it also dramatically increases their vulnerability to cyber attacks. Benefits include flexible resource management (computing, communication and storage resources are rented, normally without long-term commitments, rather than bought), specialization (the organization needs not hire server room experts, etc), and reliability. The increased exposure to cyber attacks comes from the fact that the owner/operator of the cloud platform has both physical access to the computers and access to the operating system or virtualization platform that runs the organization's cloud service. This access allows the owner to examine and modify the data of the software running on the cloud. In addition, cloud providers typically serve multiple client organizations in a given data center. Different clients typically share not only the data center, but also individual servers in it (concurrently) using machine virtualization techniques or operating-system containers. This phenomenon, called multitenancy, also dramatically increases exposure. While other tenants have less privileges than the owner/operator (it is more difficult for them to attack), they may not have any disincentive to attack. In other words, attacks by other tenants are harder to carry out but much more likely than attacks by the owner.

Clearly, efforts to secure applications running on the cloud are of paramount importance. This proposal focuses on the approach that is most likely to achieve this in practice.

Our project will explore techniques to secure cloud applications using Software Guard Extensions (SGX), a set of mechanisms (machine instructions)

that Intel plans to include in its processors starting in 2017. These mechanisms allow an application to secure (encrypt) part of its data and code. Assuming SGX works correctly and is used correctly by the programmer, this part of the application is immune against attacks, even from attacks by the operating system, virtualization layer, or a party with physical access to the hardware. In theory, SGX can be used to protect cloud.

Our project will investigate the principles that underlie SGX, what security properties the technology can deliver, and fundamental limitations in it.

STRATEGIC CYBER REASONING IN ATTACKER-DEFENDER RESOURCE ALLOCATION GAMES

AYALA ARAD, STEFAN PENCZYNSKI (UNIVERSITY OF MANNHEIM)

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. 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 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.

SHOCKS TO AND SECURITY IN THE BITCOIN ECOSYSTEM: AN INTERDISCIPLINARY APPROACH

NEIL GANDAL, TYLER MOORE (SOUTHERN METHODIST UNIVERSITY, TEXAS)

Researchers have come to realize that the cause of cyber/information security breaches is often not a failure of technology, but rather an absence of appropriate incentives. This insight has led to a proliferation of research on the economics of information security. Because of the interaction between the 'technology' and 'incentives,' such research is ideally undertaken jointly by computer scientists and economists. We believe that the recent rise in digital currencies (or cryptocurrencies) creates an opportunity to measure information security risk in a way that has often not been possible in other contexts. In this research project, we will investigate shocks affecting the Bitcoin ecosystem in order to improve our understanding of their impact and identify ways they can be better managed.

1. What are the shocks that affect Bitcoin, and when have they occurred historically? We propose to design and deploy measurement infrastructure to collect publicly available evidence of shocks, on both historical and "future" data. All data that we collect and the analysis scripts we write for the project will be publicly available in an open source format database. Regarding "future" data, the idea is to set up measurement infrastructure that could be also be used to collect data on an ongoing basis.
2. How do shocks disrupt the ecosystem, and how can their effects be measured?
   We anticipate that shocks will manifest in terms of exchange rate fluctuation, changes to the collective computational power of

mining operations, trade volume fluctuation, and variance in the bid-ask spread across exchange rates.

3. How might self-interested participants abuse cryptocurrency financial instruments to carry out deliberate shocks, and is there any evidence that such strategies are being or have been employed? Self-interested actors may exploit a range of new financial instruments to take advantage of shocks, including arbitrage, futures contracts, and cloud mining contracts. We set out to enumerate strategies for abusing cryptocurrencies following shocks, as well as devise measurements that inspect transactions for empirical evidence of abuse taking place.

We anticipate publishing two-three empirical papers and one public policy paper from this research agenda, as well as a **Database of Cryptocurrency Shocks and Measures,** as well as the associated data documenting the effect of shocks. We will design as much of the infrastructure as possible to operate on an ongoing, automated basis, so that the collection will continue beyond what is used for the scientific publications. Because public cybersecurity datasets are rare, this will provide a valuable service to the research and practitioner community.

SMART CITIES CYBER SECURITY (SCCS)

MICHAEL BIRNHACK, TALI HATUKA, ISSACHAR ROSEN-ZVI, ERAN TOCH

Our cities are in a rapid process of becoming smarter, increasingly making use of advanced technological systems that gather, process and use data about its residents and its infrastructures. Cities that enter this new brave world lack sufficient guidance on the meaning of deploying technological systems. The underlying premises of this research are that Smart cities are an inevitable process; that Information Systems are the backbone of Smart Cities and that cities are new to this cyber reality. Hence, focusing on Smart Cities Cyber Security (SCCS) is crucial to their functionality, safety, democracy and livability. Accordingly, the challenge is to develop Smart Cities that enjoy the benefits of Big Data while avoiding its pitfalls, namely, among other things, being sensitive to privacy and cyber security attacks.

Accordingly, the key research questions are:

- What are the cyber-related aspects of the Smart City?
- What are the novel vulnerabilities to infrastructure and to residents introduced by the Smart City?
- What are the tools available to municipalities in addressing the SCCS challenges?
- How would the transition to Smart Cities likely affect the legal and political structures of the city and its relationship with its residents?
- How should cities address the vulnerability and prevent cyber-attacks and other risks to the data gathered in the city's cyber systems and residents' privacy?

Accordingly, the research project investigates SCCS from several interrelated dimensions: planning, technology, social policy, local government law, and privacy law, applying diverse research methods, and aiming to offer a multi-faceted toolkit for the optimal design of SCCS.

The research is based on a theoretical and empirical study. Several Israeli cities take a leading role in developing Smart City, making them ideal candidates for an initial research. The goal is to offer multi-faceted toolkit for 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 in a single project. Hence, we focus on four interrelated dimensions, which are cornerstones (though not necessarily exclusively so) of a viable SCCS: planning, technology, local governance, and privacy.

The analysis is conducted separately and jointly, so to explore the intersections between these dimensions. The research will develop: (1) a set of tools for policy-makers and municipalities in the process of developing the smart city. The SCCS toolkit will mirror the multi-disciplinary challenges posed by Smart

Cities, providing tools to various decision-makers, i.e., planners, IT professionals, and security experts; (2) an integrative model that will serve as a basis for developing a comprehensive policy that discusses each of the four topics. This model will need to be tailored to fit the particular needs of a given city and will serve as a basis for technologies that protect the privacy and security of the city's citizens.

THE SELFISH AND CARING OF SHARING: EXPLORING THE REASONS AND PERSONAL OUTCOMES OF PUBLIC-SHAMING

YAEL STEINHART, JACOB GOLDENBERG

Public-shaming is defined as an informal punishment of an individual or a group that deviated socially or criminally, by informing the public about their actions or conduct, accompanied by criticism and expression of disapproval towards them. In recent years the spreading, availability and popularity of online social networks has given to any person the ability to initiate and take part in online shaming against any person, usually including the broadcasting of personally identifiable information about the shamed individual.

The proposed research will focus on public-shaming that runs through social networks, and that is activated against a target that allegedly acts in an immoral, unacceptable, violent or selfish way. We will focus on the reasons and personal outcomes of the 'shamers' – the people that take part in public-shaming. We emphasize the dual meaning attached to public-shaming of doing "the right thing" for society but on the same time having the potential of hurting the wrongdoer. We acknowledge the pivotal role morality plays in motivating people to take social responsibility; nevertheless, due to the duality of public-shaming, we predict that morality is not sufficient in explaining such behavior. We plan to explore the linkage between the execution of public-shaming and self-image perceptions; as well as the role of public-shaming as a self-expressive mechanism. Specifically, 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 be more likely to 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. The next step is to extend the understanding of the proposed effects both in the lab and in a framed field setting that involves real decisions and execution of allegedly online public-shaming.

We plan to better understand each of the factors that may drive and be a consequence of public shaming. In all studies, participants will be offered to join public-shaming, using either real or fictional cases. We also include measures related to social norms, morality, self-expressiveness and superiority as possible process indicators. The dependent measures will include the willingness to take part in public-shaming, as well as post shaming self-perceptions. The independent measures will differ on the following aspects: (a) usage of shaming cases of identified or un-identified wrongdoer; (b) presenting a similar or different wrongdoer; (c) manipulating the naive beliefs regarding the social norms for public-shaming; (d) inducing and (e) measuring self-image perceptions; (f) presenting a shaming case with an ambiguous vs. clear moral meaning; (g) using a company vs. a person, as the wrongdoer.

Part of the studies will be conducted in the lab, enabling to measure and manipulate self-perceptions in physical ways (such as: tall/short chairs, GSR measures). We will also run studies online both on Israeli and US populations.

In order to better understand the dynamics of public shaming, we plan to identify dissemination processes of public shaming on a highly popular large scale network (Twitter). We plan to crawl the network and its structure (i.e., nodes and ties) and use text mining in order to harvest the personal comments individuals add, run a sentiment analysis to estimate the emotional involvement and perhaps even self-esteem, if the text will be sufficiently rich.

In the future, after we will have enough knowledge about the phenomenon, we are planning to conduct a framed field experimented, which will measure actual public-shaming behaviors in a private social network.

TOWARDS A THEORY OF CYBER POWER: SECURITY STUDIES, META-GOVERNANCE, NATIONAL INNOVATION SYSTEM

LIOR TABANSKY

Cyber power is 'the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power'. Cyber security results from applications of cyber power. 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.

Based on years-long experience, we identify three relevant "softer" Social Science sub-disciplines - security studies, meta-governance, national innovation system - to integrate with "core" cyber technology fields, towards a general theory of cyber power. The research will demonstrate their analytical utility and 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.

Throughout history, superior means were never enough to secure strategic advantage. Cyber technology, together with doctrine and organization adaptation, made possible a direct, physically destructive attack on strategic targets at homeland. Critical Infrastructure (CI) are exposed to a threat scenario, which is no longer theoretical since 2010 discovery of Stuxnet. Despite awareness and technical prowess, national defense systems, first and foremost the military, have lost the ability to defend the society from external politically-motivated cyber security threat. This phenomenon is not a new one; it often had enabled historical Revolutions in Military Affairs. But Security Studies scholars have largely neglected cyber power. Unless we develop the Security Studies RMA analytical framework – even the most technologically developed states are likely to end up on the wrong side of an imminent Cyber RMA.

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

Governance – the formulation and implementation of policy in a specific policy domain by a network of numerous non-government, corporate, media actors, of which some are public and some are private – are central streams in contemporary governance theory. Cyber security solutions on a national level are essentially about governance: the challenge is to get the people and organization to alter their behavior. Traditional state-centric Governance ("old governance", "hierarchical models") public policy and administrative processes were top-down. Recent research focuses on the empiric reality: the traditional hierarchical model where collectively binding decisions are taken by elected representatives and then successfully implemented by bureaucrats within public administrations became rare. Governance theory use in cyber power was limited to Internet Governance. Public Policy research on Meta-Governance and non-traditional policy instruments will be especially applicable to complex cyber environment and must be better integrated into cyber power theory.

Political Economy: National Innovation Systems (NIS)

NIS literature emerging since the 1980s created insights on how some states grow more rapidly, adopt technologies earlier and gain competitive advantage. Current literature on NIS identified "mechanisms" rather than "places" (macro-institutional features of countries) as the core elements of innovation. Rapid Innovation-based (RIB) industries are at the core of cyber power; these require constant capacity to innovate rather than imitation and value through scale. NIS must be better integrated into cyber power theory, where technology and capacity building is the dominant concern

The research design combines literature analysis with theory building from case studies. This qualitative research method enables us to capture the complexity of the object of study. Theory building from case studies is an increasingly popular and relevant research strategy. Case studies will rapidly

contribute to theory building. We propose three case studies: one completed and two at initial stages of exploration.

a) Israeli Cybersecurity 1995-2015
b) Italy and Singapore. We plan to leverage our collaborations via TAU ICRC with respective colleagues in Italy and Singapore, to develop case studies of these two states.

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

UNDERSTANDING IP HIJACK EVENTS

YUVAL SHAVITT

Internet protocol (IP) addresses are a valuable resource of every organization. In recent years, a new kind of attack prevails in which the attacker hijacks the IP space of an organization, either a company of a public body, and exposes it to unlimited potential damage:

1. It is the first stage in man-in-the-middle attacks that can penetrate the organization firewall. This gives the malicious attacker access to the organization network for stilling valuable data, and planting Trojans and engaging local communication, e.g., using SCADA.
2. It can be used for phishing attacks that allow the malicious attacker to harvest passwords of the organization web site users.
3. It can disconnect part of the organization network from the Internet. In addition, an attacker can hijack the IP address of an organization service provider and spy on its intellectual property. This may include mail server traffic, VoIP and conference call traffic, and backup traffic. Even seemingly benign traffic such as web searches can expose future interests and technology directions. Hijacking of HTTP traffic can also enable the attacker to inject malicious code to the surfing machine inside the organization network.

Renesys (now Dyn) and other organizations identify hijack attacks by analyzing BGP announcements. While this approach is capable of detecting hijack that is based on false BGP announcement it suffers from several drawbacks. First, since they rely on BGP feeds from a limited number of sources they based their analysis on partial view of the network, and due to the intrinsic filtering of BGP it may miss many hijack events. It is suspected that many hijack events are local and their messages may thus be filtered out when propagating through the system. The other major drawback on relying on BGP announcement is that they can only detect hijack events that are based on the BGP protocol. However, there can be other ways to perform hijack, e.g., by changing a DNS server content, by inserting static entries to forwarding tables at strategic points, and by altering BGP announcement en route.

The proposed Research:

We will analyze hijack events over time, and compare active monitoring with BGP based detection. The proposal includes:

1. Building a BGP analysis tool improving previous published techniques. Identifying hijack events using data from RouteViews, RIPE, and others. Analyzing the hijack events to better understand their duration, target types, time of day, distance, etc.
2. Building a traceroute analysis tool improving previous published techniques. Identifying hijack events using data from at least two companies that already agreed to share data with us, and based on data from the DIMES project at Tel Aviv University. Analyzing the hijack events as above.
3. Comparing the two methods by identifying areas cover by both. We expect to find hijack events that are not seen by BGP and attempt to understand the technique used for the hijack. We can also use active monitoring to check if hijack at the BGP level always result in packets following the new route.

Characterizing the hijack attacks is an important block in understanding how to build a detection system, how to tune hijack anomaly algorithms, and how to automatically fight hijack events.

ULTRALONG FIBER LASER FOR SECURE COMMUNICATIONS

JACOB SCHEUER

The aim of this research is to explore fundamentally new secure information technologies in optical engineering and to develop a practical framework for the design of secure communication systems based on using an ultralong fiber laser as a transmission medium.

One of the key challenges in modern developments of information technologies is to ensure reliable and Highly secure communications for public, business and government activities. The main Achilles' heel of many of the contemporary encryption methods is that they require the two parties (Alice and Bob) to share a secret key before the secure communication can take place and in many practical scenarios this requirement is difficult to be realized. This obstacle, known as the key-distribution problem, has attracted much attention over several decades and much work has been devoted to resolve it. In particular, substantial efforts were focused on physical-layer based cryptographic protocols such as quantum key distribution, lasers synchronization in the chaotic regime, speckle pattern based optical one-way functions, and more recently – symmetry based key generation systems utilizing thermal fluctuations or ultralong fiber lasers (UFLs). Many of these physical layer encryption/key distribution schemes suffer from practical constraints which severely limit the achievable performances in terms of data-rate, range and cost. In addition, most of these schemes (including QKD) have been proven to be breakable by taking advantage of the non-ideal nature of the components comprising the scheme. The UFL key distribution scheme, which is the youngest member in this family, exhibits the greatest potential in terms of range, key-rate and cost. Very recently, UFL based secure and error-free key distribution was demonstrated over a 500km long link with key-rate of 125 key-bits per second – substantially outperforming all other physical-layer KDS. In addition, it was shown that the probability of a prospective eavesdropper, employing a variety passive attack strategies, to recover a key-bit can be reduced below 55% (where 50% indicates unbreakable scheme).

The UFL-KDS consists of a long fiber laser with Alice at one end and Bob on the other. Each of the two parties controls the reflection spectrum of one of the laser end mirrors while the laser cavity serves as a communication link between them. To exchange a bit, each party randomly selects a bit and encodes it (using his/her end mirror) into the laser. The lasing characteristics allow the two parties (and a potential adversary) to determine only whether they chose identical or opposite bits. Since each party knows his/her own bit they can deduce the other party's choice and to exchange a bit. An adversary can only deduce whether Alice and Bob succeeded in exchanging a bit, but not to determine its value. The low cost and superior performances (compared e.g. to QKD and KJLN) of the UFL-KDS render it highly attractive for practical implementation. Nonetheless, the resilience level of the scheme to cryptographic attacks should be studied more thoroughly in order to identify its potential vulnerabilities and limitation and to develop appropriate protective mechanisms. The preliminary analysis demonstrated the resilience of the UFLKDS to a wide variety of passive attacks. However, the system might be vulnerable to other attack strategies, in particular **active** attacks. Unlike passive eavesdropping where the adversary tries to extract information without altering or modifying it, actives attacks may involve external injection of (optical) power into the systems, attempts to impersonate a legitimate user (e.g. man-in-the-middle attack) etc. Active attack strategies are generally more diverse than passive ones and may require reinforcing of the UFL-KDS security. The main objectives of the proposed exploratory program are to investigate the resilience of the scheme to a variety of active attacks and to obtain quantitative metrics to information of the key that might be obtained by a potential adversary. The research will include both theoretical and experimental efforts to study the system resilience to eavesdropping and for developing appropriate countermeasures.

Although the main physical platform of the proposed research is fiber optics, the scheme can be implemented for diverse applications such as on-chip and

board to board secure communication using dielectric integrated waveguides and semiconductor optical amplifiers. Such applications are in particular attractive because of the technological maturity and relatively low cost of such components, as well as the compatibility with conventional processes for CMOS technology.

VIOLENCE AND THE (SOCIAL) CONSTRUCTION OF CYBER DETERRENCE

AMIR LUPOVICI

This research aims to develop a new framework for the study of cyber deterrence that will take into account not only traditional factors such as actors' capability and credibility, but also the social context through which each of these factors are mediated in shaping actors' behavior. A key issue in this regard is whether the means that are operated through cyberspace are constructed as means of violence.

The proposed research seeks to answer two main questions: 1) To what extent and how have countries adopted a cyber deterrence strategy? and 2) Is cyber deterrence an effective strategy-that is, does cyber deterrence affect the willingness to execute cyber-attacks?

My main argument is that an actor's retaliation is seen as more legitimate if it follows the absorption of "a violent act", and therefore an actor's deterrent threat is more credible when there is a consensus over whether the act is defined as violent. This influences both the defender (the deterrer actor), specifically, its willingness to adopt this strategy, and the putative challenger- and thus the chances of deterrence success.

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

We suggest that individuals vary in their ability to control FB cues when such cues interfere with performing goal directed activities. 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). We suggest that individuals vary in their ability to control FB cues when such cues interfere with performing goal directed activities. 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.

Our research proposal has two main advantages over prior studies: (A) We develop a novel paradigm that directly isolates the online neural mechanism of filtering irrelevant social network information, as opposed to prior findings involving overt behavior measures that can only be remotely associated with an underlying brain filtering process13-16. Importantly, we further evaluate the specificity of our underlying neural filtering predictor, by contrasting

individuals' ability to filter irrelevant FB information, with individuals' ability to filter irrelevant general information (B) We measure actual FB usage (e.g., time spent and activities) in the laboratory and in daily life, as opposed to the majority of prior studies that evaluated FB usage relying exclusively on self-report measures that are susceptible to multiple biases. Accordingly, the present research program has two main goals that will be tested in two large studies each involving 120 participants (adopting 0.8 power level, alpha =.05 and medium effect size). 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.

WHAT'S THE VALUE OF BUG BOUNTY PROGRAMS?

KEREN ELAZARI

The exploratory study aims to develop an economic model to assess the value of Vulnerability Reward (Bug Bounty) programs, in which software companies offer compensation to outside hackers who find vulnerabilities and disclose responsibly.

Research Question: What's The Value of Bug Bounty Programs?

1. Financial Value : e.g. more efficient bug discovery process
2. Business / Organizational Value: e.g. a new source for HR hiring
3. Reputational Value: e.g. company is considered "more secure"
4. Technology Value: e.g. effect of program on product feature R&D
5. Legal/ Liability Value: e.g. lower cyber insurance premium

TEL AVIV UNIVERSITY
Pursuing the Unknown

ICRC
Blavatnik Interdisciplinary
Cyber Research Center

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

www.icrc.tau.ac.il