SEMINAR SUMMARY

APRIL 2019

ENHANCING CYBERSECURITY:
THE ROLE OF INNOVATION ECOSYSTEMS

MIT innovation initiative

CYBER SECURITY
RESEARCH CENTER
Cyber Law Program

האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

סייבר ישראל
Cyber Israel
מערך הסייבר הלאומי - משרד ראש הממשלה
National Cyber Directorate - Prime Minister's Office

Department for
Digital, Culture,
Media & Sport

UK Science
& Innovation
Network

EXECUTIVE SUMMARY

This document summarizes the conversations from the seminar "Enhancing Cybersecurity – The Role of Innovation Ecosystems" that took place on February 13th 2019 at the Massachusetts Institute of Technology in Cambridge, Massachusetts.

The goal of the Seminar was to advance participants' knowledge of innovation ecosystems for innovation in cybersecurity. Its approach was to emphasize the growing agglomeration of innovation-driven enterprises creating innovative solutions, and the tightly-coupled inter-dependencies in these hubs of entrepreneurs, governments, risk-capital, universities and large corporations.

The Seminar was organized by the **MIT Innovation Initiative (MITii), the Federmann Cyber Security Center at the Hebrew University of Jerusalem (HCSRC), Israel's National Cyber Directorate (INCD), the UK Department for Digital, Culture, Media & Sport (DCMS), and the UK Science & Innovation Network.** Forty participants representing all of the ecosystem stakeholders (governments, universities, corporations, entrepreneurs, and risk capital) were invited to participate (see Appendix B).

The Main Insights:

- Cybersecurity is an area of technological, corporate and regulatory innovation that emphasizes the growing agglomeration of innovation-driven enterprises and inter-dependencies between entrepreneurs, governments, risk-capital, universities and large corporations. **Innovation ecosystems thus provide an important lens to understand the specific case of innovation in cybersecurity, and to enhance our understanding of innovation ecosystems in general**.

- This insight is key for practitioners and promoters of innovation in cybersecurity, as the lessons from wider 'innovation ecosystems' become more and more relevant to their efforts. **As such, the multi-stakeholder ecosystem approach** (broadly defined) **can help enhance and accelerate innovation in cybersecurity**, as it has elsewhere**.**

- The conversations at the Seminar underlined specifically the value of innovation ecosystems for **mitigating the asymmetry between offensive and defensive cyber capacities, providing appropriately-skilled workers and continuous training, institutionalizing the interaction between stakeholders, bridging cultural gaps, and developing a common professional language**.

- The Seminar concluded that it is necessary to **further advance our understanding of cyber innovation ecosystems and their value for enhancing cybersecurity**. The organizers will therefore **initiate an international comparative analysis of selected existing cyber innovation ecosystems**.

1. THE SEMINAR AND ITS GOALS

Cybersecurity – defined as the practice of defending cyber infrastructures such as computers, servers, mobile devices, and IoT devices; as well as the data itself, from attack - is a mission of great importance. Its change is being driven by increasing digitalization of human activities that not only improves lives, but also increases vulnerability to cyberattacks on, for example, infrastructure, banks, hospitals, factories, and homes. Today's estimates of the financial damage caused by cyberattacks are around $3 trillion annually, but by 2021 they will likely have risen to over $6 trillion. For governments, this is reflected in steadily increasing budgets for cyber defense: according to World Bank estimates, by 2030 a total of 0.5 percentage of the world GDP will be used on cybersecurity. Thus, effective cybersecurity is about protecting our everyday lives, the resilience of industry and commercial services, and the functionality of our societies in an increasingly digital world.

The Seminar's underlying hypothesis was that cybersecurity would (perhaps paradoxically) be amenable to the same multi-stakeholder ecosystem approach which MIT concludes that other forms of tech innovation are demonstrating; i.e., an approach that emphasizes the growing agglomeration of innovation-driven enterprises creating innovative solutions and the tightly coupled, inter-dependencies in these regions of entrepreneurs, governments, risk-capital, universities and large corporations. The need to enhance and accelerate cybersecurity innovation is driven by the low (and dropping) price of cyber weapons, the high (and rising) capabilities of various actors with nefarious intentions, as well as the need for more rapid security responses. As such, it is important to assess the conclusion that the ability to provide cybersecurity will depend on interactions within cyber-focused innovation ecosystems among the diverse stakeholders mentioned above.

Some examples of such ecosystems around the world are the Be'er Sheva-based 'CyberSpark' in Israel, Kendall Square and greater Boston in the US, and both Belfast and London in the UK – just to mention a few. At the same time that these ecosystems have moved ahead with improving cybersecurity for their stakeholders, **the full role of cyber innovation ecosystems in so doing is still a phenomenon that needs to be further understood, analyzed and developed.**

Against the background of this understanding of the critical role of regional innovation ecosystems and the hypothesis that they will provide key insights and best practices for enhancing cybersecurity, four institutions have come together around the common project of deepening this understanding; eliciting critical elements for the success of such ecosystems; and following up with research into specific case studies and models. Thus, the **MIT Innovation Initiative (MITii), the Federmann Cyber Security Center at the Hebrew University of Jerusalem (**HCSRC)**, Israel's National Cyber Directorate (INCD), the UK Department for Digital, Culture, Media & Sport (DCMS), and the UK Science & Innovation Network** came together to undertake three main goals:

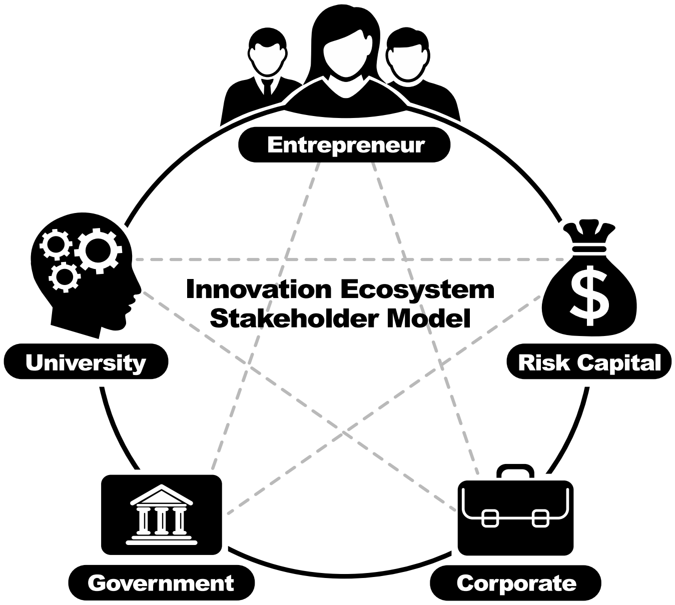
- To advance our knowledge of innovation ecosystems and how they apply in meeting the challenge of cybersecurity;
- To define and share best practices through a comparative analysis of selected cyber innovation ecosystems;
- To provide analysis on how the critical relationships among diverse stakeholders in such ecosystems may be improved.

The February 2019 seminar was a first step towards achieving these common objectives. The invitation-only event gathered representatives from governments, entrepreneurs, corporations, universities and risk capital to explore current best practices and relations among the stakeholders in such cyber-focused innovation ecosystems. This document summarizes the keynote presentations, various conversations and the takeaways of this Seminar.

2. MIT’S FIVE STAKEHOLDER-MODEL FOR INNOVATION ECOSYSTEMS

The Seminar opened with a presentation by Prof. Fiona Murray (MIT) and Dr. Phil Budden (MIT) on MIT’s five stakeholder model for Innovation Ecosystems. The presentation underlined that innovation-driven activity today is highly concentrated in key global locations. Research shows that, within highly concentrated geographic regions, innovation-driven activity is also characterized by significant agglomeration and exchange of resources, strongly grounded in teams building high-growth, innovation-driven enterprises. These so-called ‘innovation ecosystems’ are multi-stakeholder in nature, with critical roles for government, private corporations, risk capital providers, entrepreneurs and universities.

Figure 1: MIT’s Five Stakeholder Model for Innovation Ecosystems



Given the multi-stakeholder and cross-sectoral nature of cybersecurity, innovation in this field is likely to thrive in such innovative ecosystems.

The success of cyber innovation ecosystems – as with other innovation ecosystems - depends on the capacity to efficiently transition ideas to impact (often in the form of new successful innovation-driven enterprises who may later partner with large corporations for distribution and service provision) which is enabled through a diverse set of programs and policies implemented by the system's five main stakeholders. Such actions may include the creation of accelerators, talent development programs, testbeds to evaluate new solutions, academic-industry centers of excellence, and new or revised policies to protect intellectual property rights.[1] These programs often target five critical areas - human capital, funding, infrastructure, demand, and culture/incentives – which together advance the capacities for innovation and entrepreneurship of the ecosystem (in the current case, for cybersecurity) and address any frictions within it that negatively impact these capacities or the mobility from one part of the ecosystem to another. These frictions may exist among the stakeholders due to different cultures and approaches to governance; yet may also be caused by the lack of sufficient, patient risk capital, insufficient talent or infrastructure and the like. Examples of actions that have already targeted different tensions in such ecosystems include the Charter of Trust by Siemens, the Cybersecurity Factory by Highland Capital Partners, and the Workforce Talent Challenge by The MassCyberCenter.

The presentation of MIT's five stakeholder-model at the outset of the seminar thus underlined for the participants the importance of an innovation ecosystem approach for understanding the specific case of innovation in cybersecurity and enhance our understanding of innovation ecosystems in general. This opening laid the foundations for the conversations throughout the seminar about the actions and strategies of the different ecosystem stakeholders and the challenges for which they seek to find the right solutions.

[1] For further reading, see: "A systematic MIT approach for assessing 'innovation-driven entrepreneurship' in ecosystems" by Phil Budden and Fiona Murray.

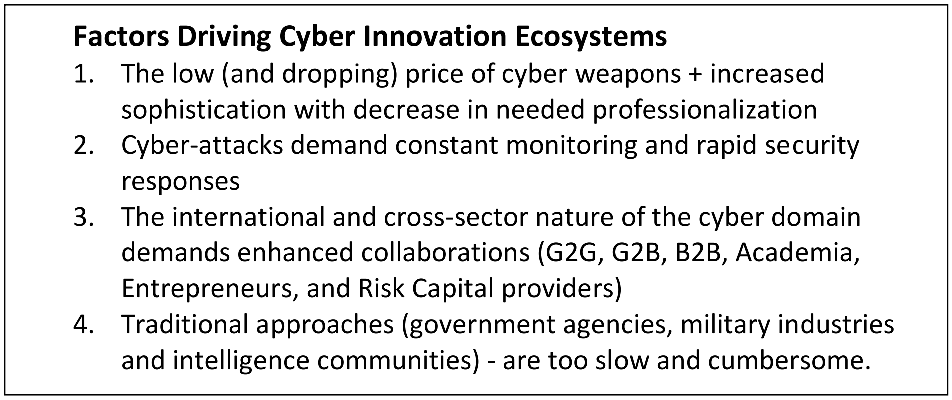
3. THE RELEVANCE OF INNOVATION ECOSYSTEMS FOR CYBERSECURITY

In the second presentation, Dr. Amit Sheniak (Hebrew University) presented an overview of how and why cybersecurity challenges today demand organizational changes by states and companies, in order to be able to develop better technologies for cyber defense. Basing the presentation on his article entitled "Not merely a Technological Advantage: The United States' Organizational Change in Cyber Warfare",[2] he proposed that the growing reliance on increased financial investment in cybersecurity innovation as the primary policy taken by states and organizations,[3] is insufficient: rather, organizational change is needed that will open the boundaries of government-centric solutions to include other stakeholders. The significance of focusing on organizational and conceptual change, and not solely on technological development and investment in order to achieve a security advantage in cyberspace, is based on two complementary factors:

1) the increasing number of cyber-attacks and the changes in their aim, scope and mechanisms (see Table 1 below); and

2) the growing sensitivity of other technologies (including weapons systems) to cyber-attacks due to their growing interconnectivity and reliance on computer mediated communication.

Factors Driving Cyber Innovation Ecosystems



Factors Driving Cyber Innovation Ecosystems

1. The low (and dropping) price of cyber weapons + increased sophistication with decrease in needed professionalization
2. Cyber-attacks demand constant monitoring and rapid security responses
3. The international and cross-sector nature of the cyber domain demands enhanced collaborations (G2G, G2B, B2B, Academia, Entrepreneurs, and Risk Capital providers)
4. Traditional approaches (government agencies, military industries and intelligence communities) - are too slow and cumbersome.

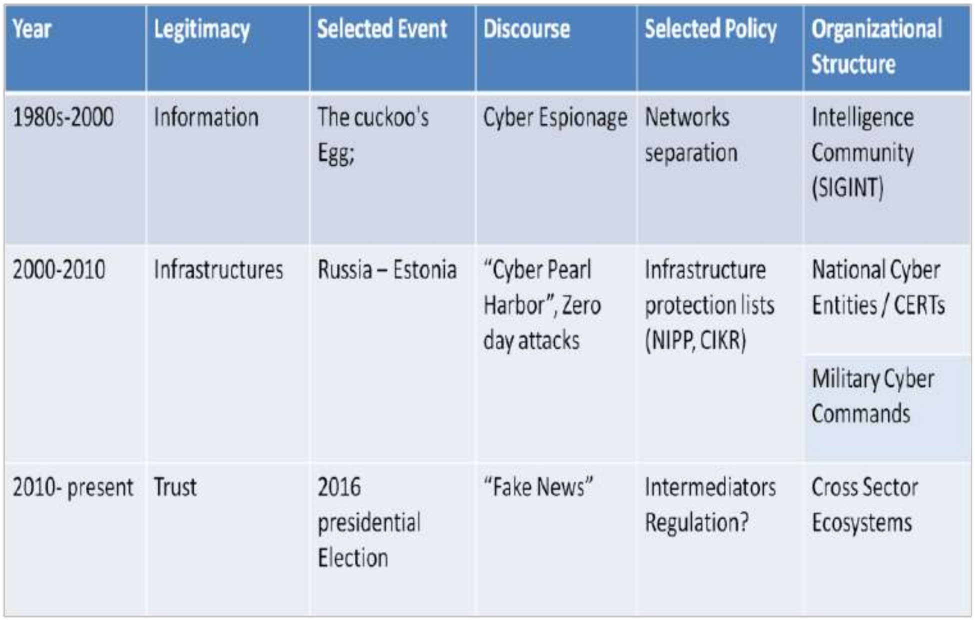
[2] Sheniak A. (2017). " Not merely a Technological Advantage: The United States' Organizational Change in Cyber Warfare" Cyber, Intelligence, and Security, Volume1, No.3 (December)

[3] See for example the Obama administration's policy to increase cybersecurity innovation funding with a supplement of 19 billion US Dollars. Tobias Naegele, "7 Keys to President Obama's 19 Billion Cybersecurity Plan," *GOVTECH Works*, February 16, 2016, https://www.govtechworks.com/7-keys-to-obama-19-billion-cybersecurity-plan/#gs.iMSThHM.

As Table 1 indicates (see below), the rise of computer-enabled attacks, from the mid 1980s until today, highlights the organizational changes of the US defense establishment to mitigate the growing effectiveness of cyber-attacks to security in general and to modern technology in general. These changes led to an accumulated change in the perception of cyberspace, that can be described in three stages:

1. From the 1980s until 2000, cyber challenges were perceived as a threat to sensitive information, such as official state information, intelligence, and intellectual property, thus they were defined as “information security”;
2. Between 2000 and 2010, cyber challenges were also perceived as a threat to basic infrastructure and critical resources needed for modern states' sustainability - which could be defined as "civil/national defense";
3. Finally, from 2010 until today, cyber-challenges were also perceived as threats to states' sovereignty and to interpersonal interactions (economic, political, and social) of its citizens, hence a threat to "public security".

Table 1: The Change in Cybersecurity Legitimacy and Organizational Structure



Year	Legitimacy	Selected Event	Discourse	Selected Policy	Organizational Structure
1980s-2000	Information	The cuckoo's Egg;	Cyber Espionage	Networks separation	Intelligence Community (SIGINT)
2000-2010	Infrastructures	Russia – Estonia	“Cyber Pearl Harbor”, Zero day attacks	Infrastructure protection lists (NIPP, CIKR)	National Cyber Entities / CERTs Military Cyber Commands
2010- present	Trust	2016 presidential Election	“Fake News”	Intermediators Regulation?	Cross Sector Ecosystems

These unique characteristics led to the conclusion that the ability to mitigate vulnerabilities in cyberspace cannot be based solely on technological development, which tends to be designed for each sector separately and to rely on the regular national research and development mechanism (such as military industrial complexes). [4] Hence, it must also include new public and private organizational structures, doctrine and proficiencies that exercise policy in a manner that integrates between the public and the private sectors, increasing the pace of innovation and improving user's efficiency. These understandings are already implemented in the creation of national Computer Emergency Readiness Teams (CERTs) – a form of program that is key to enhancing innovation ecosystems in this and other domains -integrating intelligence and operational pictures from both governmental and private entities, and with semi-governmental bodies that mediate between the public and private sectors.[5] It is also evident in the "multi-stakeholder" approach for advancing international voluntary cyber-norms.[6]

In most cases, states acknowledge that they cannot compete with the pace of the development in the private market (as well as the relatively low prices of malware and malicious cyber tools), and the fact that progress sometimes requires long-term, basic research in fields such as cryptology, artificial intelligence and other advanced forms of computation. Therefore, cyber innovation ecosystems that serve as a hub connecting different stakeholders from different sectors, have come about as new organizational and institutional approaches to the rapid and agile development of innovative solutions to cyber-challenges and as a preferable cyber-security approach. Growing in number and typologies, and chosen as the typical national solution to contemporary cyber challenges, cyber innovation ecosystems work a "relay station" that connects different relevant stakeholders.

[4] The US administration recognized this problem a decade ago. See, for example, "Securing the Nation's Critical Cyber Infrastructure," (2008). p. 3, Figure 1.

[5] For example, the US: National Computer Security Center (NCSC); National Infrastructure Advisory Council (NIAC); Information Sharing and Analysis Center (ISAC).

[6] See Savage J.E. and McConnell B.W. (2015). "Exploring Multi-Stakeholder Internet Governance". *EastWest Institute*. (January). https://www.eastwest.ngo/sites/default/files/Exploring%20Multi-Stakeholder%20Internet%20Governance_0.pdf

4. SUMMARY OF THE KEYNOTES, PANELS AND GROUP WORK

The presentations of Prof. Fiona Murray, Dr. Phil Budden, Dr. Amit Sheniak, and Dr. Lars Frølund were followed by keynotes from David Shores (INCD) and Jonathan Darby (DCMS); then two panel discussions with representatives of all the ecosystem stakeholders; and finally, cross-stakeholder group work. This design of the day enabled all participants to present their point of view.

Three questions guided these conversations:

- In what ways are innovation ecosystems around the world important for you, and how would you describe your current engagement with them? For example, are your ways of engaging with innovation ecosystems a “one size fits all” approach, or do you use different modes of engagement for each innovation ecosystem with which you interact?
- What are the critical frictions that you encounter in trying to develop solutions for cybersecurity - at the national level, and at the trans-national level? For example, are there specific regulatory hurdles that need to be addressed, cultural "clashes" between worldviews among various sectors, or other gaps that innovation ecosystems might help to minimize?
- Once frictions have been mitigated - what are the success factors specific to the cybersecurity mission?

Generally, all of the seminar participants pointed to cyber innovation ecosystems as a needed outset of cooperation to enhance cybersecurity. The following section presents cross-cutting takeaways from the conversations.

Multi-stakeholder Collaboration

Stemming from the basic characteristics described above, a few specific challenges were elucidated that encourages states to enhance their innovation in cybersecurity through multi-stakeholder collaboration:

- **Use cyber innovation ecosystems to accelerate the pace of innovation.** The rate of the development of malware and vulnerability discovery, alongside the expansion of the digitalization of services and industries (i.e. medico-tech, transportation, fintech etc.) is one of the prime reasons for the establishment of innovation ecosystems focused on incentivizing entrepreneurs and risk capital to increase their pace of innovation.

- **Mitigate asymmetry through innovation ecosystems.** The known asymmetry between offensive and defensive cyber capacities was mentioned as a primary source of concern for states and corporate representatives that participated in the seminar, and as an incentive for the creation of hubs of expertise that have the potential of narrowing that gap.
- **Create deterrence through cyber innovation ecosystems.** The latter were described as the most important (and possibly the only) sources for leverage against attackers and a possible source for the creation of deterrence effect against cyber attackers.

Workforce Resources

A known challenge, the lack of skilled personal that are able and willing to work in the cybersecurity sector, was mentioned as an example of a common difficulty that can be improved through an innovation ecosystem approach:

- **Provide skilled workers**. The ability of different innovation ecosystems to provide skilled workers that are looking for professional experience (such us university students, or local workers), such as in the case of the Beer-Sheva cyber-park that is part of the Ben-Gurion University computer engineering campus, is one of the common reasons and benefits of cyber innovation ecosystems.
- **Cybersecurity demands constant training, new technologies, and information sharing**. Ecosystems have the ability to create the needed common institutions that can accommodate that need, whether by employing joint training programs, leaning on the academic and professional stakeholders' expertise. Or the sharing of information of cyber-attacks and threats, collected by government representatives and institutions such as national CERTs.
- **Ecosystems' local culture and branding matter**. The local setting of some of the ecosystems mentioned with their unique cultural and symbolic essence (i.e. social-economic status), together with available transportation, housing, social institutions and more, are part of the appeal that attracts both companies and skilled work-force to choose to be a part of them.

Trust

The inability to contain the social/political mistrust inherent in many of ICTs tools, and digitalized information in general (partially caused by some of the contemporary types of cyberattacks that distort data and information), and cultural and professional language gaps, was a main issue emphasizing the importance of ecosystems to enable trust among the stakeholders**:**

- **Institutionalize interaction among stakeholders.** The need to institutionalize interaction among the stakeholders through, for instance, vetting institutions, regulation, standardization was mentioned as collective actions that could advance trust with regard to suppressing cyber-related issues such as supply-chain security and the security of Internet-of-Things (IoT) tools. Innovation ecosystems are seen as the right place and possible "test bed" to such trust-enabling mechanisms especially by corporations and government representatives, as they require the intensified interaction among the different stakeholders to be able to develop the mechanisms and legitimize their use
- **Bridge cultural gaps.** The need to bridge cultural gaps was not only mentioned by several participants, but were also very evident in the interactions between the different stakeholders participating in the Seminar. These gaps were due to the different personal and national backgrounds, and different professional training such as: intelligence, policy, computer engineering, or management.
- **Develop a common cyber-language**. The use of undefined terms and professional lingo among the stakeholders emphasized the need for a common and commonly-understood vocabulary of cyber-related terms.

5. THE NEXT STEPS

An International Comparative Analysis of Cyber Innovation Ecosystems

It is necessary to further advance our understanding of cyber innovation ecosystems with **a focus on their frictions and how to better resolve them.** The organizers will therefore initiate an **international comparative analysis of cyber innovation ecosystems**. The analysis will comprise in depth analysis of activities, programs and policies from all ecosystem stakeholders with a focus on the areas mentioned above.

The execution of the analysis will be led by representatives from HCSRC (chair), MIT, INCD, DCMS, and additional organizations representing entrepreneurs, corporations, and risk capital. The **results will be disseminated through two main channels:**

- **Presentations in conferences and panels** – The results of the Seminar and the scope and aim of the comparative analysis will be presented at the DCMS-led event "Encouraging a Thriving, Innovative Digital Security Industry" in London November 2019 (co-organized with the OECD). The final comparative analysis and recommendations will be presented at an international conference in Israel organized by The Hebrew University Federmann Cyber Security Center in conjunction with the INCD in the second half of 2020.

- **Publications** – policy and research papers will include the first international comparative report on cyber innovation ecosystems, that will include in-depth and elaborated description of the research findings and a possible additional theoretical model that will serve as part of future training and educational programs.

END

Enhancing Cyber Security: The Role of Innovation Ecosystems

February 13, 2019 | MIT ILP Conference Center

MIT
innovation
initiative

CYBER SECURITY
RESEARCH CENTER
Cyber Law Program

האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

Prime Minister's Office
National Cyber Directorate

UK Science
& Innovation
Network

INTRODUCTION

Cyber security is a mission of great importance worldwide. For governments, this is reflected in increased budgets for cyber defense: according to World Bank estimates, by 2030 a total of 0.5 percentage of the world GDP will be used on cyber security. This change is being driven by increasing digitalization that not only improves lives, but also increases vulnerability to cyberattacks on, for example, infrastructure, banks, hospitals, factories, and homes. Today's estimates of the damage caused by cyberattacks are around $3 trillion annually, but by 2021 they will have risen to over $6 trillion. Thus, effective cyber security is about protecting our everyday lives and the functionality of our societies in an increasingly digital world.

The low (and dropping) price of cyber weapons as well as the need for more rapid security responses, has led governments to the conclusion that the ability to control and defend cyberspace, demands enhanced collaboration between government and private actors such as universities, entrepreneurs, large corporations, and risk capital. We refer to such multi-stakeholder approaches as key to an innovation ecosystem approach in cyber security.

Organized by the MIT Innovation Initiative, Cyber Security Research Center at the Hebrew University of Jerusalem, Israel National Cyber Directorate, and UK Science and Innovation Network, the seminar will address the following questions:

- What are the current best practices of an innovation ecosystem approach relevant to cyber security?
- What success factors for the cyber mission can be developed from ecosystem best practices?
- How can we create impact by translating the best practices and success factors into initiatives such as advanced training courses, training guidelines, and professional and academic publications?

AGENDA

8:30 am	**Breakfast & Registration** *(MIT ILP Conference Center)*
9:00 am	**Welcome** • **Fiona Murray**, MIT Sloan School of Management
9:15 am	**Goals of the Seminar** • **Dr. Lars Frølund**, MIT Innovation Initiative • **Dr. Amit Sheniak**, Hebrew University of Jerusalem
9:45 am	**Innovation Ecosystems and Stakeholders** • **Prof. Fiona Murray**, MIT Sloan School of Management • **Dr. Phil Budden**, MIT Sloan School of Management
10:15 am	**Keynote & Q&A** • **David Shoresh**, Israel National Cyber Directorate *(keynote)* • **Dr. Amit Sheniak**, Hebrew University of Jerusalem *(moderator)*
11:00 am	**Coffee & Networking**
11:15 am	**Panel: Best Practices from Corporations** • **Andy Ellis**, Akamai • **Tristan Morgan**, BT Security • **Natalia Oropeza**, Siemens AG • **Parisa Tabriz**, Google • **Dr. Lars Frølund**, MIT Innovation Initiative *(moderator)*
12:30 pm	**Lunch & Networking**
1:30 pm	**Keynote & Q&A** • **Jonathan Darby**, UK Department for Digital, Culture, Media & Sport *(keynote)* • **Dr. Phil Budden**, MIT Sloan School of Management *(moderator)*
2:15 pm	**Coffee & Networking**
2:30 pm	**Panel: Best Practices from Entrepreneurs and Risk Capital** • **Sam Curry**, Cybereason • **Sean Dalton**, METEOR VC • **Galina Antova**, Claroty • **Deborah Housen-Couriel**, Hebrew University of Jerusalem *(moderator)*
3:45 pm	**Coffee & Networking**
4:00 pm	**From Insights to Impact** *Group work addressing questions on how to further develop our knowledge and create impact.* • **Dr. Lars Frølund**, MIT Innovation Initiative *(moderator)* • **Dr. Amit Sheniak**, Hebrew University of Jerusalem *(moderator)*
5:15 pm	**Closing Remarks** • **Prof. Fiona Murray**, MIT Sloan School of Management • **Deborah Housen-Couriel**, Hebrew University of Jerusalem • **David Shoresh**, Israel National Cyber Directorate • **Jonathan Darby**, UK Department for Digital, Culture, Media & Sport
6:00 pm	**Informal Dinner** *(MIT ILP Conference Center)*

SPEAKERS

Galina Antova

Claroty

Galina Antova is the Co-Founder and Chief Business Development Officer at Claroty. Prior to co-founding the company, she was the Global Head of Industrial Security Services at Siemens, leading the Cyber Security Practice and Cyber Security Operations Center, which provided managed security services for critical infrastructure customers.

Previously, Galina was with IBM Canada, with roles in the provisioning and cloud solutions business. She holds a BS in computer science from York University in Toronto, and an MBA from the International Institute of Management and Development in Lausanne, Switzerland.

Phil Budden

MIT Sloan School of Management

Phil Budden is a Senior Lecturer at MIT's Management School, in Sloan's TIES (Technological Innovation, Entrepreneurship and Strategic-management) Group, where he focuses on 'innovation-driven entrepreneurship' (IDE) and innovation ecosystems.

Phil co-teaches in the successful 'Regional Entrepreneurship Acceleration Program' (REAP), an ExecEd program for regional teams from around the globe interested in accelerating 'innovation-driven entrepreneurship'; in the related 15.364 class, known as the 'Regional Entrepreneurship Acceleration Lab' (REAL), aimed at MBAs and Sloan Fellows; and on similar topics in a variety of degree and ExecEd settings.

Phil's approach combines academic, historical and real-world perspectives on how different stakeholders — including Entrepreneurs, Universities and 'Risk Capital' providers, alongside Corporate enterprises and Government policymakers — can all contribute to building successful innovation ecosystems. He is currently on leave from the British Government, and joins MIT having worked recently in Boston's private sector for the Royal Bank of Scotland's US subsidiary, Citizens Bank, where he focused on financing transatlantic (especially British-American) trade and investment. His background as a diplomat makes him well-suited to the 'global innovation' of REAP/REAL, the interplay among the REAP teams, and the negotiations within the 'innovation ecosystems' (especially between Corporate and Government stakeholders).

Sam Curry

Cybereason

Sam Curry, Chief Security Officer at Cybereason, is an IT security visionary with over 20 years of IT security industry experience. Sam served as Chief Technology and Security Officer at Arbor Networks, where he was responsible for the development and implementation of Arbor's technology, security, and innovation roadmap.

Previously, he spent more than seven years at RSA (the Security Division of EMC) in a variety of senior management positions, including Chief Strategy Officer and Chief Technologist and Senior Vice President of Product Management and Product Marketing. Sam has also held senior roles at Microstrategy, Computer Associates, and McAfee.

Sean Dalton

METEOR VC

Sean Dalton is a co-founding partner of METEOR VC, an early-stage firm dedicated to partnering with compelling enterprise technology entrepreneurs with a vision to build important companies. Based in Boston, METEOR leads "true Series A" rounds, providing teams company-scaling support in partnership with the 50+ members of the METEOR Network and METEOR Domain Experts — a group of successful founders, CEOs, influential executives, and technology experts.

Sean has led investments in over 20 enterprise and wireless companies, including Starent (IPO and $2.9B acquisition by Cisco). He currently serves on the boards of ClearSky Data, Exagrid, and Xometry and is a seed investor in a number of emerging "Cloudscale" enterprise companies. He is a co-founder of the Cybersecurity Factory, a program focused on seed-stage intellectual property in security and blockchain.

Sean has been selected to the *Forbes* Midas List multiple times as one of the top venture capitalists in the country. *Business Insider* named him one of the "15 Most Powerful Venture Capitalists on the East Coast." Prior to METEOR, Sean served as a managing general partner of Highland Capital Partners from 2005 to 2018. Sean started his career as a product manager for GTE (now Verizon). Sean holds an MBA from HBS, an MSEE from Penn, and a BSEE from University of Delaware.

Jonathan Darby

UK Department for Digital, Culture, Media & Sport

Jonathan Darby is Head of Cyber Growth and Innovation at the UK Department for Digital, Culture, Media & Sport, a role he has held since November 2017. His home department is the Foreign Commonwealth Office (FCO) and he has undertaken diplomatic postings in Singapore and Chicago. He also worked for the Victorian Government, Melbourne, Australia.

Prior to joining the FCO, Jonathan worked in the telecoms industry, for Orange and P&O. He has a LLB from Cardiff University and an MBA from the Open University. He is from Carmarthenshire in West Wales.

Andy Ellis

Akamai

Andy Ellis is Akamai's Chief Security Officer, and his mission is "making the Internet suck less." Governing cybersecurity, compliance, and safety for Akamai's planetary-scale cloud platform since 2000, he has also designed and brought to market Akamai's TLS acceleration network, its DDoS defense offerings, and several of the core technologies behind its security solutions. Andy has also guided Akamai's IT transformation from a flat password-based network to a distributed, zero-trust enterprise based on strong authentication.

Andy is a graduate of MIT with a degree in computer science, and has served as an officer in the United States Air Force with the 609th Information Warfare Squadron and the Electronic Systems Center.

Also active in Internet policy and governance circles, Andy has supported past and present Akamai CEOs in roles on the NIAC and NSTAC, as well as serving on the FCC's Communications Security, Reliability, and Interoperability Council.

He is an affiliate of Harvard's Berkman Klein Center, and a guest lecturer in executive education at MIT and the Harvard Kennedy School. He is a frequent speaker on topics of Internet security, anthropocentric risk management, and security governance; and occasionally blogs at csoandy.com. He can be found on Twitter as @csoandy, where he discusses security, wine, American football, and hairstyling.

Lars Frølund

MIT Innovation Initiative

Dr. Lars Frølund is the Research Director of the MIT Innovation Initiative and a Visiting Fellow at MIT Sloan School of Management. His research focuses on the success factors for university-industry partnerships in innovation ecosystems, mission-driven research and innovation, and the role and value of intermediaries. He is the co-editor of the book Success Factors for University Partnerships where leading companies describe their excellence in industry-university collaboration.

Recently, he has worked with Professor Fiona Murray (MIT Sloan) and Dr. Max Riedel (Siemens) on the six questions a company must ask itself to develop a systematic approach to university partnerships in innovation ecosystems. The paper, "Developing Successful Strategic Partnerships with Universities," was published by *Sloan Management Review*. He was a Fulbright Scholar at MIT Sloan from 2016 to 2017.

Deborah Housen-Couriel

Hebrew University of Jerusalem

Deborah Housen-Couriel's expertise focuses on global and Israeli cybersecurity law and regulation. Her law practice advises clients on high-level strategies for legal planning and regulatory compliance in the areas of corporate governance, preparedness, data protection, and cybercrime. She also works closely with Konfidas Digital, a leading Israeli cybersecurity and data protection consulting firm. Deborah's experience at the international level includes her current service as Chair of Working Group D of the Global Forum on Cyber Expertise, as a Core Expert on the Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS) project, and as a member of two of the GCSC's Research Advisory Groups. She was a member of the International Group of Experts that drafted the 2017 Tallinn 2.0 manual on state activity in cyberspace.

Deborah is an advisory board member of the Hebrew University Cyber Security Research Center; and a research fellow at the Minerva Center for the Rule of Law under Extreme Conditions; IDC Herzliya's Institute for Counter-Terrorism; and the Interdisciplinary Cyber Research Center at Tel Aviv University. She teaches courses on cybersecurity law and regulation at the Law School of Hebrew University and at the Herzliya IDC, and has served as a guest lecturer at the Harvard Kennedy School's Exec Ed Program on Cybersecurity: The Intersection of Policy and Technology.

She is currently researching regulatory models for government-private sector information sharing to mitigate cyber threats.

Tristan Morgan

BT Security

Tristan (Tris) Morgan is the Chief Technology Officer of BT Security. Tris has 15 years' experience working across both the enterprise and 5EYES community providing innovative and groundbreaking cyber security capability.

In his current position, he is responsible for the technology portfolio end-to-end: from running the highly successful security innovation programme through to leading the technical capability teams in delivery. Tris has also worked with Silicon Valley start-ups, down streaming their capability into the security sector.

Prior to this, Tris held multiple roles with BT, including as an advisor to senior government stakeholders on technical strategy, Chief Architect for cyber solutions, and running operational teams.

Tris graduated with a BSC (Hons) in computer science with artificial intelligence.

He is married with two young children and enjoys skiing and sailing in his spare time.

Fiona Murray

MIT Sloan School of Management

Fiona Murray is the Associate Dean of Innovation at the MIT Sloan School of Management, William Porter (1967) Professor of Entrepreneurship, and an associate of the National Bureau of Economic Research. She is also the co-director of the MIT Innovation Initiative. Professor Murray is an international expert on the transformation of investments in scientific and technical innovation into innovation-based entrepreneurship that drives jobs, wealth creation, and regional prosperity. She has a special interest in the commercialization of science from idea to impact and the mechanisms that can be effectively used to link universities with entrepreneurs, large corporations, and philanthropists in that process.

She serves on the British Prime Minister's Council on Science and Technology and has been awarded a CBE for her services to innovation and entrepreneurship in the UK.

Natalia Oropeza

Siemens

Natalia Oropeza has more than 27 years of experience in the area of information technology, consisting of several leadership positions, international experiences, as well as broad experience in technical roles.

Natalia began her career at Volkswagen de Mexico, and undertook several diverse roles including a PBX, Communication Specialist, and also as a Network Team Leader for gedas Mexico.

In 1997, Natalia took on her first international assignment as a Network Project Manager at Volkswagen Headquarters in Wolfsburg, Germany. In 2001, she was promoted to the Network and Customer Services Manager for VW America. In 2004, she returned to Mexico to work as the Enterprise Operations Director for gedas. In 2006, she took on a role as Vice President of IT Operations for T-Systems International GmbH in Munich in order to broaden her professional experience. In 2011, she returned to the VW Group in Wolfsburg to lead a global IT security initiative, ITSP, and after successful delivery of the project, was promoted to Chief Information Security Officer for the entire Volkswagen Group.

Natalia led the largest IT Transformation Program for the VW Group, in which she reported directly into the VW Group Board. In her current position, she is leading cybersecurity for Siemens combining the topics protection of infrastructure (IT/OT), protection of products, solutions, and services, as well as enabling cybersecurity offerings for customers.

Amit Sheniak

Hebrew University of Jerusalem

Dr. Amit Sheniak is the Cyber Security Policy Coordinator of the Israeli Ministry of Defense political-military directorate. He is also a post-doctoral research fellow at the Hebrew University of Jerusalem, Davis Institute for International Relations, Truman Institute for the Advancement of Peace, and a research fellow at the Hebrew University Cyber Security Research Center.

Dr. Sheniak holds a MA and PhD in political science from the Hebrew University of Jerusalem and a post-doc from the Harvard Kennedy School Program for Science, Technology and Society. He had served in the past decade as a Chief Policy Advisor and Strategy Analyst in various capacities at Israel's parliament, the ministry of defense, and the Israeli Defense Forces.

His research and publications investigates the social and political context of state-sponsored innovation technologies, specifically in regard to cyber security conflicts, cyber-policy and expertise formation and their effect on international order, sovereignty, and legitimacy in the Middle East, US, and China.

David Shoresh

Israel National Cyber Directorate

David Shoresh is strategic planner at the Israeli National Cyber Directorate (INCD). He is responsible for strategic assessment, policy setting on national cyber security affairs, and the INCD multi-year plan.

He previously served as a strategic planner in the IDF General Staff (J5), where he was involved in a wide range of politico-military issues, operational planning and force development. Prior to that he was a legal advisor in the IDF Military Advocate General Corp. He is an award winning writer on strategy and technology.

Parisa Tabriz

Google

Parisa Tabriz is a Director of Engineering at Google, currently responsible for making Chrome the most safe, stable, and useful tool for browsing the web across all your devices. She also manages the Project Zero team, is affectionately known as Google's "Security Princess" (her former job title!), and has worked on information security at Google for over a decade, starting as a "hired hacker" software engineer for Google's security team. As an engineer, she found and closed security holes in dozens of Google's web applications, and taught other engineers how to do the same.

Outside of Google, Parisa has lectured at the Harvard Kennedy School, served as a consultant to the White House US Digital Service to enhance security of government technology, and consulted with multiple entertainment writers to help them understand the world of cyber security and technology so they can create and depict more accurate, diverse stories.

ACKNOWLEDGEMENTS

ORGANIZING COMMITTEE

Lars Frølund
MIT Innovation Initiative

Phil Budden
MIT Sloan School of Management

Fiona Murray
MIT Sloan School of Management

Amit Sheniak
Hebrew University of Jerusalem

Deborah Housen-Couriel
Hebrew University of Jerusalem

David Shoresh
Israel National Cyber Directorate

Dadi Gertler
Israel National Cyber Directorate

Ronit Prawer
UK Science & Innovation Network

THANK YOU

MIT Industrial Liasion Program

MIT Innovation Initiative
Massachusetts Institute of Technology
One Broadway, 12th Floor
Cambridge, MA 02142

> **innovation.mit.edu**
> **innovation@mit.edu**

Enhancing Cyber Security – The Role of Innovation Ecosystems

List of Participants

Name	Organizaton
Alan Halachmi	Amazon
Amit Sheniak	The Hebrew University of Jerusalem
Andy Ellis	Akamai
Ben Brabyn	Level 39
Bradley Finn	UK Department for Digital, Culture, Media & Sport
Christian Wentz	Gradient Tech
Dadi Gertler	Israel National Cyber Directorate
Dan Trajman	NEIBC
David Shoresh	Israel National Cyber Directorate
Deborah Housen-Couriel	The Hebrew University of Jerusalem
Fiona Murray	MIT
Gal Gnainsky	Philips
Gali Levakov	Israel National Cyber Directorate
Gene Keselman	MIT
Godfrey Gaston	Queen's University Belfast
Hamed Okhravi	Lincoln Lab
Herve Coureil	Schneider Electric
Jens Erik Dalsgard	Office of the Danish Tech Ambasador
Jonathan Darby	UK Department for Digital, Culture, Media & Sport
Justin Lakamper	Konrad Adenaur Foundation
Kathryn Person	MIT
Katie Stebbins	University of Massachusetts, President's Office
Kevin Quinlan	MD5
Lars Frølund	MIT
Michael Siegel	MIT
Michelle Lampa	Trade and Investment, British Consulate
Mike McGinley	Defense Innovation Unit
Natalia Oropeza	Siemens
Padraig Maloney	BAE Systems / Fast Labs
Parisa Tabriz	Google
Peter Lewis Clasen	Belfer Center
Phil Budden	MIT
Rafi Yayalom	MIT
Ravi Pappu	In-Q-Tel
Rick Miles	Red Seal
Ronit Prawer	UK Science & Innovation Network
Sally Guenette	Philips
Sam Curry	Cybereason
Sean Dalton	METEOR VC
Stefan Just-Dummer	Siemens
Stephanie A. Helm	MassCyberCenter
Steve Whittaker	British Telecom
Steven Palmer	MIT
Tristan Morgan	British Telecom

CYBER SECURITY
RESEARCH CENTER
Cyber Law Program

האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

MIT innovation initiative

סייבר ישראל
Cyber Israel
מערך הסייבר הלאומי - משרד ראש הממשלה
National Cyber Directorate - Prime Minister's Office

UK Science
& Innovation
Network