Enhancing Cyber Security – The Role of Innovation Ecosystems

February 13th, 2019

Initial Report

1. General

1.1 The low (and still-falling) price of cyber weapons, as well as the need for more rapid security responses, has led many governments to the conclusion that their ability to protect national assets (both military and civilian) in cyberspace and to mitigate the risks and impact of hostile activity in this domain demands enhanced collaboration between government and private actors, such as universities, entrepreneurs, large corporations, and risk capital organizations. Such multi-stakeholder approaches are key to an *innovation ecosystem approach* to cyber security (hereafter ICE).

1.2 The MIT Innovation Initiative (MITii), the Federmann Cyber Security Research Center (Law Program) at the Hebrew University of Jerusalem, the Israel National Cyber Directorate (INCD), and the UK Science and Innovation Network are collaborating to explore this new ICE approach in a series of events and knowledge-creation trajectories. Our first meeting took place at MITii in the form of a one-day seminar that addressed the following questions:

- What are the **current best practices** for an innovation ecosystem approach relevant to cybersecurity?
- What **success factors for bolstering cybersecurity** can be developed from innovative ecosystem best practices?
- How can we **create positive impact** by translating best practices and success factors into initiatives that increase cybersecurity awareness and preparedness, such as advanced training courses, training guidelines, and professional and academic publications?

1.3 The seminar was by invitation only, and participants came from top-tier organizations in government, academia, large corporations, and risk capital organizations (see Appendix A for a full list of participants).

2. **Methodology** (see Appendix B for the full seminar schedule)

2.1 The seminar kicked off with presentations discussing the applicability of the five stakeholder ecosystem model that was developed by MITii in the field of cybersecurity

innovation. This model emphasizes the important addition of entrepreneurs and investors to the better-known and more prevalent collaborations between government, academia, and large corporate actors. The seminar than continued with the presentations by various stakeholders sharing their extensive experience, in the format of both moderated keynote lectures from government representatives (Israel / INCD, UK / Department of Digital, Culture, Media and Sport) and panels. The two panels included one presenting corporations (Siemens, British Telecom, Google, and Akamai) and another showcasing entrepreneurs and risk-capital (Level 39, Cybereason, Red Seal and Meteor).

2.2 The seminar also included many opportunities for networking, and concluded with a session of group work that gave many of the additional participants (i.e. non-speakers) a chance to share their knowledge and experiences. The group participants were asked to discuss both frictions and best practice ideas regarding the relationships between the different stakeholders in the ecosystem.

3. **Initial insights** – the discussion that followed the panels, and especially the group work, stimulated the curation of some initial insights and thoughts regarding the characteristics of cyber innovation ecosystems, as follows:

3.1 **The nature of the cyber threat emphasizes the need for collaboration:** The rapid development of malware and vulnerability research, alongside the expansion of the digitalization of services and industries (i.e. medi-tech, transportation, fintech etc…), is one of the prime reasons for the establishment of an innovation ecosystem focused on cybersecurity. The asymmetry between offensive and defensive cyber action experienced by governments and big corporations encourages them to enhance their innovation attempts, whether internally or, more commonly, by incentivizing entrepreneurs (mainly start-ups) and investors to increase their pace of innovation. Hence, innovative activities, enterprises, and initiatives are considered by cybersecurity professionals in governments

and corporation to be the most important resource for leverage against attackers and a potential source for the creation of deterrence.

3.2 **Culture and language gaps:** These gaps were explicitly mentioned by several participants, but were also very evident while observing the interactions between the different stakeholders participating in the workshops. Whether due to different personal and national backgrounds, different professional training (intelligence, policy, computer engineering, and management, to name just a few fields) or the use of blurred and undefined controversial terms and professional lingo, there is clearly a need to create and institutionalize interaction between the stakeholders, using these frictions as an engine for improvement and growth and motivating the participants themselves to emphasize the need for a common and commonly-understood vocabulary of cyber-related terms.

3.3 **Trust:** The inability to contain the social / political mistrust inherent in many of ICTs tools, and in digitalized information in general (partially caused by some of the contemporary types of cyberattacks that distort data and information), is another issue that highlighted the need for joint mechanisms that might enhance trust (i.e. vetting institutions and procedures, standardization, norms proposal, and implementation). These mechanisms were mentioned as a key incentive for the creation of cybersecurity innovation ecosystems, especially by big corporation and governments representatives, as they require intensified interaction between the different stakeholders in their development, and most importantly in legitimizing their use.