

Witness Statement

Offered on 28 July 2010 to the House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities (TUTC), for the hearing entitled, *Harnessing Small Businesses Innovation for National Security Cyber Needs*.

Contributor:

John H. Ricketson
CEO, Dejavu Technologies, Inc.
D'Angelo Drive, Marlborough, MA 01752
508-281-2527
jricketson@dejavutechnologies.com

Personal CV

For the last two years I have managed Dejavu Technologies, a start up software technology company focused on network forensic analysis for cyber security. For over 30 years I have worked in high technology. As a corporate buyer for Dynatech Corporation during the 1980s, and most recently as an independent consultant for 15 years prior to my current position, I have personally managed over 40 equity financial transactions involving small companies in industrial technology markets. I have a BSEE from Princeton University in Electrical Engineering and Computer Science, and an MBA from the Harvard Business School.

Prior Entrepreneurship

Dejavu's operating team and angel investor group have been serial entrepreneurs. Dejavu is the fourth sequential start-up technology company associated with this team. I was personally involved in the most recent two ventures. Each prior venture was successful, and sold to large technology product companies. These companies started as commercial customers and became strategic buyers, acquiring the product lines to include in their own portfolio. The prior ventures were as follows: ClearSpring Technologies (acquired by Veritas/Symantec), Synthetic Networks (acquired by Agilent), and Imperfect Networks (acquired by Spirent). Dejavu is our first venture that has been primarily focused on government markets, so we have experienced a steep learning curve.

Cyber Security Technology

The *TrafficScope* technology created by Dejavu is a comprehensive network forensic analysis tool. Simply stated, TrafficScope allows an analyst to "Google" network history looking for any clues to discern the nature of newly uncovered cyber threats, and to trace what damage might have been done, and what assets might be most vulnerable.

TrafficScape is a very innovative product in many ways. A key innovation is to capture and store network content utilizing search engine technology, rather than a traditional relational database. As a result, TrafficScape stores pre-analyzed free-form data that may be rapidly searched for any arbitrary item of interest, plus relationships among items. TrafficScape can scale to handle huge quantities of stored forensic data.

Another innovation is the *ePersona* feature, which uses search engine technology to rapidly recall cross-reference relationships. This is a productivity tool for cyber investigators.

TrafficScape uses the underlying search engine to reconstruct views of complex http traffic and Web 2.0 applications. For example, TrafficScape is able to trace botnet machines use of social network sites to communicate with their masters, as was documented with the Ghostnet cyber attacks uncovered last year.

TrafficScape is at a very early stage, the first version having been released early this year. We have only one direct government contract, but other units purchased and on evaluation loan to integrators and cyber security consulting firms.

Small Business Agenda

Dejavu is a small company with a big idea. Thus, Dejavu is an example of small business as a fountainhead for out-of-the-box thinking and innovative ideas for solving the world's most important problems. The challenge for an innovative company like Dejavu is to get the big idea heard by the agencies who should care, because the new technology might further their mission.

Government policy regarding small business has many noble goals, but "innovation" is fairly low on the priority list. The major goal is economic growth and job creation. A secondary goal is to provide opportunity for disadvantaged groups or geographies. Most of the government programs I have seen support those goals. However, support for technical innovation is more difficult to find.

Innovation and Cyber Security

Cyber security is an arms race, with effective defenses spawning newer and more creative threats. There will never be a perfect shield, nor a silver bullet. Dejavu has focused on the forensic problem, because discerning and researching new threats will be a perpetual challenge.

As a nation we must understand that encouraging innovation is key to tackling the cyber security challenge. In fact, this challenge is actually an opportunity for government to experiment with more and better ways to encourage technical innovation.

Anecdote: a trip to my local SBA office

We work closely with technical groups within a large systems integrator, and I wanted to further that relationship. When I heard SBA provides support for large systems integrators to "mentor" small innovative companies, I made an appointment with the SBA office in Massachusetts. I immediately discovered the "mentor" program was an 8a set-aside, for which we did not qualify. However, the SBA representative proudly showed me their full list of SBA programs. While all were worthy, none were helpful to us:

- Mentor – 8a set-aside.
- SBA loans through local banks – requires a personal guarantee plus asset collateral, or specific contracts with cash flow needs.
- SBIC equity through local VC firms – no different from other VCs.
- SBIR technology grants – 1-2 year process, applying to each agency.
- Hubzone – targets geographical areas we are not in.
- PTAC (procurement assistance to match our skills to government agencies) – not designed for high technology, but for service contracting firms.
- Consulting advice about business plans – not needed for us.
- Contracting Assistance – not needed for us.

Anecdote: What Stimulus Money?

Stimulus money was in the headlines for many months last year. I was amused by the words "shovel ready" to mean projects that could be implemented immediately. Because of our prior technology ventures, we have an extended network of highly qualified engineers, local in Massachusetts, unemployed or doing consulting work. We could put them to work "immediately" building advanced cyber security products, for which we know there are government requirements. I had limited time bandwidth to seek such money, and I was unsuccessful at finding any.

Hindrances to innovation (and some constructive suggestions)

Software Certification. Certification and accreditation of software is a requirement for many agencies. There are very good reasons, of course. However, this is a significant hurdle for small innovative companies. The going rate for outside consultants to manage this is about \$100,000 plus 6-12 months of time. It would be helpful if there were government money, or a free government-sponsored service, to move promising products through this process.

Security Clearance. Many cyber security programs require security clearances for a full discussion of technical requirements and innovations. Security clearance requires a sponsor to take a direct interest. Policies to facilitate this process would be helpful.

Technical intermediaries. There are technical consulting organizations, whom government agencies rely upon for objective answers about new technology. MITRE is a good example. Rather than wait for specific government sponsor request, it would be helpful if such organizations were given charter and funding to validate the claims of new and innovative products. Objective validation of technical claims, and comparison of a variety of creative solutions, is a valuable service to both the vendor and the government sponsor.

Outreach programs. Some agencies have created a department for handling outreach to new, small companies. In our experience, very good examples are the ARC registration process and intro sessions at both NRO and Ft Meade, and also the DHS S&T industry outreach program. These departments attempt to function as gatekeepers, to potentially link new firms with technical sponsors within the agency. More funding for these activities would be welcome, especially if there were ways to measure such productivity, and if more funding assures that personnel have technical qualifications which allow them to be credible to both outside firms and to the agency experts they serve.

Tax policy. Finally, it is obvious to point out that we would like to be rewarded for this hard work, at the end of the day. Therefore, it is very discouraging to hear about raising the long-term capital gains tax for equity that we entrepreneurs hold.

Conclusion

Government policies in support of technical innovation should promote a wide variety of technology ideas to compete openly, rather than attempt to pick technology winners. In this respect, government should be wary of trying to emulate the VC industry, whose mission is to make good returns on their money, rather than to solve the world's most important problems. Competition for new solutions should have a level playing field of information. A little chaos is a good thing. Given a chance, in the form of attention, time, and money, the best ideas will rise to the top.