Cyber Security Summit 2014 – Documentation of the working groups

Working Group 3: Encouraging Innovation in Cyber Security

The public sector has a responsibility

Germany invests too little in cyber security innovations. Startups often struggle to obtain the capital they need in order to bring their ideas to the market. And the public sector has not been promoting digital technology innovations by coming forward as a lead customer.

There is too little willingness in Germany, and in Europe in general, to invest in security innovations. There is a complete lack of an innovation culture such as that seen in Silicon Valley (U.S.), or in Tel Aviv (Israel), the world's second-largest center for innovation. Silicon Valley companies annually provide an estimated 15 billion euros of venture capital. In Tel Aviv, such investments amount to about 1.7 billion euros per year. By contrast, investors in Germany annually provide less than 700 million euros of venture capital.

In this light, it is not surprising that innovators often look abroad. Anyone who wants to turn a good idea into business has virtually no option but to look abroad for venture capital. Germany certainly has no lack of smart minds and good ideas. But because of a lack of capital, and of a low willingness to take risks, on the part of investing companies and the public sector alike, not as many innovative products and technologies are developed here as could be developed in terms of the available inventive talent.

Investors in Germany often slow innovation by focusing too much on risk minimizing and cost reduction before the actual task – the implementation of an innovative idea – has been achieved. That can suffocate startups and nip good ideas in the bud. Investors often refuse to even consider taking a stake unless an innovator can prove he will have a mature product within two years.

Successful examples of startups show that such caution and impatience are not necessarily justified: For example, the startup company Pinterest collected

a total of 750 million dollars, from a range of different capital providers, over a four-year period. Since its last round of financing, it has been valued at 5 billion dollars. And yet it is unclear when that company is going to start turning a profit. Another startup, Flipboard, which was founded in 2010, acquired about 100 million dollars in two rounds of financing, and is now valued at about 800 million dollars. In the digital society, anyone who has a good idea has to bring it to market fast even if it's going to take years to become profitable.

"Companies with truly great ideas won't find financing at the local savings bank."

A startup in Germany, after painstakingly courting investors, might be lucky to generate venture capital of 500,000 euros. But that is simply too little to get a company off the ground. What is more, entrepreneurs often have to accept starting capital at the cost of allowing investors to take overly large stakes. Their motivation suffers if the financing process leaves them with only 10% of their own company. To succeed, an innovator has to be passionate about his company and his idea. If investors crowd him out, his commitment will suffer – and that will endanger his success.

The culture of investment in Germany needs to change in the interest of innovation in Germany. For example, enough capital for innovations could become available if companies would simply allocate one percent of their purchasing budgets to buying from startups. In addition, the public sector should take a considerably larger role, also in providing venture capital. In Silicon Valley and Tel Aviv, security innovations are often financed by the military or by government security organizations. Germany's and Europe's public sectors also need to be making the investments that will make innovative security products possible.

And of course industry has the task of making the market more aware of the threats in cyberspace. Companies need to collaborate to that end. They need

to share information about security incidents – even though, as we all know, no one wants to admit he has been the victim of an attack.

What is needed are more transparency, a greater willingness to take risks and a significantly higher commitment to venture-capital financing.