Authors: Reinder Wolthuis, senior consultant/projectmanager at TNO. Marth Breure, innovation analyst at TNO Vector and Ruggero Montalto, projectmanager at TNO. Authors to be reached at reinder.wolthuis@tno.nl, marth.breure@tno.nl and ruggero.montalto@tno.nl

Security innovation and tech transfer

Security innovation is done by many organizations and is essential to protect society against advanced cyber-attacks. But these innovations are useless unless they are also applied in practice. The Dutch cybersecurity innovation community currently experiences a tech transfer gap, where innovation results don`t always find their way into actual products and services available on the market. This article assesses the prominent reasons why this gap exists and proposes potential solutions to reduce it.

The Partnership for Cybersecurity Innovation (PCSI, www.pcsi.nl) is a collaboration among TNO, ABN AMRO, ING, ASML, Achmea, and the Netherlands Tax Administration (Belastingdienst).

PCSI has the ambition to collaboratively innovate on cybersecurity by producing innovative technical, process, or methodological results. These innovation results are intended to improve the protection against cyber-attacks both for the PCSI partners and the Dutch community.

PCSI has been striving to produce results that will be used in practice by the PCSI Partners and the Dutch community after an innovation project has been finalised. This ambition could not be sufficiently fulfilled until now for several reasons. PCSI clearly experiences a 'tech-transfer gap' in between innovation and the actual adoption and use of the result.
The broader Dutch cybersecurity innovation community also experiences a tech transfer gap, where innovation results not always find their way into actual products and services on the market. One of the instruments that the Ministry of Economic Affairs and Climate Policy (EZK) has implemented to support this topic is dcypher, a collaboration platform for research and development on cybersecurity in the Netherlands (1).
Since EZK has a high interest in the success of tech-transfer of innovation results, they awarded a project to TNO to find potential solutions that could reduce the tech transfer gap for the PCSI as well as the Dutch cybersecurity innovation community.

A resulting report, specifically addressing the PCSI tech transfer, has been published earlier this year (2) and a more generic report on tech transfer for the Dutch cybersecurity innovation community will soon be published. Results have been gathered from literature, interviews with relevant stakeholders, and workshops.
The tech transfer gap is graphically represented in Figure 1, showing a combination of the Market Readiness Level and the Technology Readiness Level:

- TRL – the Technological Readiness Level scale measuring the maturity of a technology being developed by a project.
- MRL – the Market Readiness Level scale measuring the commercial readiness of a technology in respect to the market.

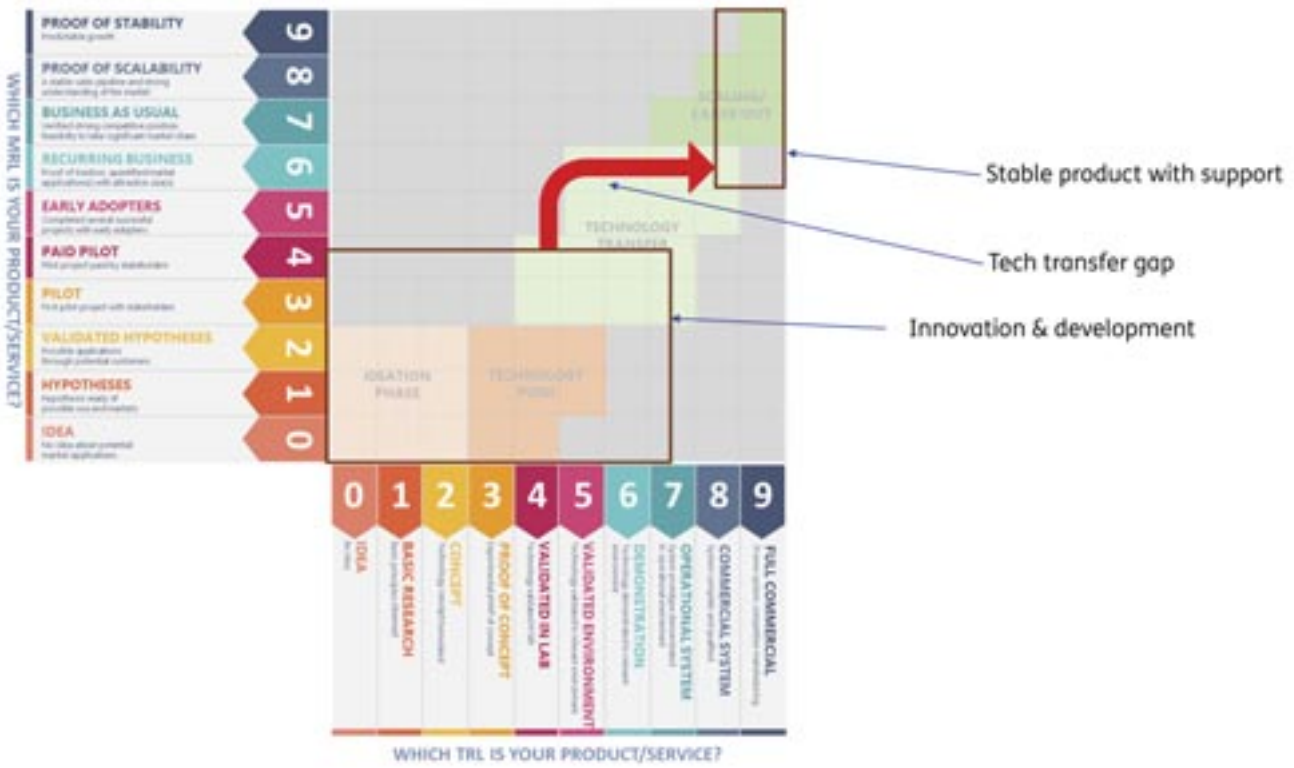

Figure 1: The tech transfer gap from the perspective of TRL and MRL level.

As Figure 1 shows, innovation projects usually produce results at TRL 6-7 and MRL 4. A product needs to be at TRL 9 and MRL 6-7 in order to be considered mature and suitable for the market. The tech transfer gap is the difference between these two stages for innovation projects. Ideally, this gap is not present, and a solution finds its way to market in an uninterrupted manner. But, more often than not, this is not the case.

Tech transfer barriers

One of the main findings from our research is that the maturity of the cybersecurity ecosystem in the Netherlands is relatively high. The Netherlands has a thriving educational cybersecurity environment and mature research and knowledge institutes (doing well on TRL levels lower than 5). The Netherlands also has an active government, mature investigation services, and a high number of companies that are active in the cybersecurity field. However, transforming good ideas and innovative results into products and services that can be used in practice remains to be a difficult journey. In particular, from the information gathered it seems that the number of Dutch start-ups with cybersecurity technologies or services is low compared to what one sees in other countries.This is due to the harshness of the entrepreneurial climate, Dutch culture, the inherent difficulty of the cybersecurity target market, regulatory and entry-level barriers, and a limited workforce with the right expertise.

Within the Dutch market, large end users of cybersecurity solutions tend to focus on large suppliers with proven track record and product suites that offer a multitude of functionalities. They prefer to buy off the shelf systems. Although understandable from a supplier management perspective, this hinders the introduction of small start-ups that often focus on a specific technology and are not stable companies yet. The lagging demand for Dutch alternatives for these global products also means that the knowledge, IP and technology is bought, instead of developed.

The lagging demand can also be accounted to the smaller size of the Dutch national market for cybersecurity products compared to the demand in market of other countries. This

When users know their needs and can articulate them to entrepreneurs, better cooperation and better fit products arise

smaller demand than neighbouring countries such as France, the Baltic countries, the U.K. and Israel, is in part to be explained by the lower impending sense of danger or of lack of threat experienced by an imminent cyber-attack of a foreign actor. This also explains why the US and Israel have such large demands for cybersecurity.

Culturally, the Dutch prefer avoiding investing in the development of long-term, disruptive and innovative cybersecurity solutions due to the high risk and delayed ROI associated with long term R&D. The lack of funding and market opportunities leads Dutch entrepreneurs to sell their innovative cybersecurity start-ups to foreign buyers (often American or Israeli) or even avoid investing in innovative cybersecurity to begin with. This means that the acquired IP and knowledge, also leaves the country. Entrepreneurs seem to work from a short-term ROI perspective instead of a long-term Cybersecurity self-sufficiency vision.

Competition in commercial bids is also a barrier for the tech transfer of innovative cybersecurity products: Requests for Proposal (RFPs) focus on competition and do not facilitate cooperation and demand articulation. When users know their needs and can articulate them to entrepreneurs, better cooperation and better fit products arise. Moreover, Venture capital investors on one hand are usually interested in products with their own intellectual property rights, and therefore prefer funding technology focused cybersecurity companies. The Dutch market on the other hand is mostly interested in service oriented cybersecurity companies.
Another aspect is that cybersecurity products are usually not mass-market products. But the lesser customization a cybersecurity product requires, the higher the potential ROI will be and consequently the chances to attract potential investors will be higher.

Also, EU laws and regulations (e.g., the requirement of GDPR compliance) complicates market introduction, especially when components are included that come from outside the EU.
Finally, start-up technology often needs to integrate or collaborate with tools and technology already prevalent in the market. This integration usually takes considerable effort that could slow down the actual implementation of innovative cybersecurity solutions.

The barriers experienced in the Netherlands are in line with what we find in literature: the lack of entrepreneurial competency and attitude within academia has been frequently highlighted (7,8), as has the need for better market research and increased connection with the market (3). Another factor described in literature is the lack of long term substantial financial support while the return on investment on innovative cybersecurity products is insecure (5). This is exacerbated by the extended development and resource requirements (11), and the high degree of uncertainty and risk associated with high-tech innovation (6, 10, 11).

Potential solutions

Although most solutions to solve the tech transfer gap in the literature are often difficult to turn into realistic business cases, there are some easy steps suggested in literature; optimizing the support and trainings from the technology transfer office and to add an experienced business coach to mentor the spin-off (5). Another suggestion is involving non-academic business colle-

By separating the activities, the disconnect between academia and entrepreneurs can be avoided

agues with previous experience in the industry (4) and strong work ethic/motivation in the core team as a surrogate entrepreneurial from an early phase onwards (9). Finally, extra emphasis is put upon the necessity of a ROI analysis (10, 11).

Aligning academic and industry goals in a common language while understanding the sector differences is not easy. Not all academics and entrepreneurs are able to switch ways of working so immediate. Recent literature on high-tech transfer suggests splitting the activities in two (3); a technology-focused development stage under the lead of academia and an application-oriented stage headed by entrepreneurs. By separating the activities, the disconnect between academia and entrepreneurs can be avoided. Academics are highly skilled in the development stage and technical proficiency, but they often lack the skills necessary for successful technology commercialization in the application stage, such as entrepreneurial capabilities, familiarity with industrial use-cases, and access to venture capital. With the separation, the tech-transfer can be improved by letting the researchers focus on the technology and transferring the final development steps and commercialization paths not only through spin-offs, but primarily through licensing to existing or newly founded companies.

From the interviews we learned that headway in the desired direction (decreasing the tech transfer gap) can be made by stimulating the entrepreneurial climate in the Netherlands. This would require:

- A clear vision of the demand articulation of the market, supported by economic anchors (large companies that can strengthen an entire ecosystem, e.g., the semiconductor industry around ASML) that change and support the entire landscape with their demand.
- More availability of risk capital on the market, which requires a change of mind set on investors and tax support measures. Strategically engaging investors should be brought in when there is a functioning TRL 6 prototype.
- Support by the Dutch government with advice (e.g. availability of tech transfer coaches), (pre-) competitive finding, positive investment climate, guidelines to stimulate the market.
- Willingness of end users (both government and private companies) to buy and use products from start-ups.
- A preference to buy products from EU start-ups by (EU) governmental agencies.
- Sufficient availability of security expertise (by education and/or attracting expertise from abroad).
- Less regulatory pressure for start-ups and entrepreneurs.

Also, more innovation collaborations should be set-up, such as the PCSI. E.g. a PCSI like collaboration on Operational Technology or product security. Collaboratively, the scale of work, available knowledge and resources can be used more efficiently and barriers can be overcome more effectively.

For start-ups, the availability of unbiased and high quality information and knowledge is important but not always easy to obtain. Easy access to e.g. knowledge institutes, academia, and relevant databases should be arranged for start-ups.

Establishing a (virtual) demonstration platform for products could streamline the tech-transfer process, serving as a repository for innovation and a "shopping window" for interested commercial parties (whether those may be potential investors, security vendors or end-users).

To be maximally effective, practical solutions to the tech transfer gap problem should have a systemic approach; for instance, it is advisable to have tech transfer 'in mind' from the beginning when researching or working on cybersecurity innovation at a low/medium TRL. In practice, that means having a solid knowledge of the current cybersecurity market, as well as a properly outlined mapping of the relevant key-stakeholders. These include (but are not limited to) end-users (both people using the product and people responsible for purchasing a product), investors, open-source projects and communities, government representatives, but also marketers, legal- and innovation experts. Investors are more ready to invest in an idea for a new innovative product that really solves a problem of an end-user instead of a pure technology driven product.

With respect to commercial bids, it would help if end-users both in the private sector and the public sector start tenders with a Request for Information (RFI) instead of a RFP, lowering the focus on competition and facilitating cooperation and demand articulation instead.

Finally, since the take-over by non-EU organizations of successful Dutch companies (some of which are funded with subsidies) is a real challenge, leveraging the new Veiligheidstoets investeringen, fusies en overnames (VIFO) regulations could improve the rate of retention of Dutch start-ups. The VIFO can in fact prevent the foreign acquisition of a company when the product or services the company sells are important for the strategic autonomy and the economic security of the Netherlands.

The solutions described above all focus on commercially driven tech transfer. But security tech transfer could also profit from Open Source models, which are in essence not commercially driven. This will facilitate collaboration and exchange of knowledge.

References

(1) Dcypher website

(2) PCSI tech-transfer, Improving the applicability of PCSI innovation results, Reinder Wolthuis, Marth Breure, Ruggero Montalto, 2024

(3) From Building Block to Application: A Deep Tech Commercialization Framework, Halecker and Dotzel, 2023. www.proquest.com/docview/2840810979?pq-origsite=gscholar&fromopenview=true

(4) Accelerating a Technology Commercialization; with a Discussion on the Relation between Technology Transfer Eciency and Open Innovation, Wahyudi Sutopo, Rina Wiji Astuti and Retno Tanding Suryandari, 2019. Journal of Open Innovation. www.mdpi.com/2199-8531/5/4/95

(5) Spin-Off Strategy and Technology Transfer Office: Cases in Sweden, S. Adesola, S. Datta, 2020. doi.org/10.1007/978-3-030-48013-4

(6) Development of a Life Cycle Model for Deep Tech Startups, G. Schuh, B. Studerus, and C. Hämmerle, 2022. Journal of Production Systems and Logistics, Volume 2 article 5 d-nb.info/1253580243/34

(7) Firms' Genetic Characteristics and Competence-Enlarging Strategies: A Comparison between Academic and Non-Academic High-Tech Start-Ups. Colombo, Massimo G., and Evila Piva, 2012. Research Policy, Volume 41, Issue 1 Elsevier. www.sciencedirect.com/science/article/pii/S0048733311001673

(8) Academic Networks in a Trichotomous Categorization of University Spinouts, Nicolaou, N. and S. Birley, 2003. Journal of Business Venturing 18, 333–359 www.sciencedirect.com/science/article/pii/S0883902602001180

(9) Bridging the Bubbles: Connecting Academia and Industry in Cybersecurity Research Rasha Kashef et al, 2023. Presented during the Rogers Cybersecure Catalyst webinar series in November 2022. rshare.library.torontomu.ca/articles/preprint/Bridging_the_Bubbles_Connecting_Academia_and_Industry_in_Cybersecurity_Research/24132645

(10) The DeepTech Investment Paradox: a call to redesign the investor model. Portincaso, M. Gourevitch, A., de la Tour, A., Salzgeber, T. and Hammoud, T., 2021. Boston Consulting Group & Hello Tomorrow

(11) Context perspective on University-Industry Collaboration processes: A systematic review of literature. Nsanzumuhire, S.U. and Groot, W., 2020. Journal of Cleaner Production, 258, p. 120861. doi.org/10.1016/j.jclepro.2020.120861