TNO innovation for life

Lessons learned from PCSI and more

Security Innovation & Tech-transfer in the Netherlands

ICT, Strategy & Policy
www.tno.nl
+31 88 86 63 741
Reinder.wolthuis@tno.nl

TNO 2024 R11495 – August 2024

Security Innovation & Tech-transfer in the Netherlands

Lessons learned from PCSI and more

Authors	Reinder Wolthuis, Marth Breure, Ruggero Montalto
Classification report	TNO Publiek
Number of pages	30
Number of appendices	3
Customer	Fadime Keçe - Ministry of Economic Affairs
Project name	PCSI tech-transfer
Project number	060.55221

Contents

1 Introduction

1.1 Context

The Partnership for cyber security Innovation (PCSI, see Appendix C) is a collaboration among TNO, ABN AMRO, ING, ASML, Achmea, and the Dutch Tax Administration (Belastingdienst). PCSI has the ambition to collaboratively innovate on cyber security by producing innovation results of technical, process, or methodological nature,

One of the key ambitions of PCSI is to ensure that results from innovation actions continue to be used after an innovation project has been finalized. This ambition could not be sufficiently fulfilled until now, due to various known and unknown reasons. We have concluded that there is a 'PCSI tech-transfer gap' between innovation and the actual adoption the results.

Because successful tech-transfer of innovation results is of significant interest to the Dutch Ministry of Economic Affairs[1] (EZ), it commissioned a project to TNO to examine potential solutions to reduce this transfer gap for PCSI. The resulting report [23] summarised the results of this project, and provides recommendations for PCSI to reduce tech-transfer gaps.

The broader Dutch cyber security innovation community is well familiar with the tech-transfer gap, with many innovation efforts not finding their way into actual products and services. This is confirmed by the recently published book 'Security Innovation stories: 20 koplopers over innovatie in het cybersecuritydomein' [24]. One of the instruments that EZ has implemented to support on this topic is e.g. dcypher, a collaboration platform for research and development on cyber security in the Netherlands.[2] To ensure that the Dutch Society also profits from PCSI-specific results as described in [23], EZ asked TNO to prepare specific dissemination activities and results that ensure that learnings are shared with the broader security innovation community in Dutch society. This concise report is one of these results.

1.2 Goal

Ensure that PCSI learnings on reducing the security innovation tech-transfer gap are shared with the broader Dutch security innovation community.

1.3 Methodology

With the PCSI-specific report [23] as a starting point, we have stripped off the results that could not be generalized to the broader Dutch cyber security community. We then went once again through all the raw information (e.g. interview notes) that we gathered for the first report and we conducted additional interviews (see 0). The information gathered in the steps above was analysed in a qualitative manner to extract the main developments that are relevant for this report.

[1] The name of the ministry changed as of July 1st 2024 from Ministry of Economic Affairs and Climate Policy to Ministry of Economic Affairs, see also https://www.rijksoverheid.nl/actueel/nieuws/2024/07/02/kabinet-schoof-beedigd
[2] https://dcypher.nl/

1.4 Reader guide

Chapter 2 describes the Tech-transfer gap and learnings from the perspective of literature, and describes the barriers that stand in the way of successful exploitation of innovation. This chapter also lists a number of potential solutions to overcome these barriers.

Chapter 3 wraps up the report with conclusions and recommendations. As a management summary, reading chapter 1, section 2.1 and chapter 3 should suffice.

2 The Tech-transfer gap

In this chapter, we start with a definition of tech-transfer from the perspective of 'Marketing and Technology readiness level' in paragraph 2.1. In paragraph 2.2, we highlight some of the relevant learnings on tech-transfer from literature. Paragraph 2.3 describes the barriers as experienced by the different interviewed parties that deal with tech-transfer and luckily, also solutions were proposed to reduce the tech transfer gaps, which are described in paragraph 2.4.

2.1 Tech-transfer in terms of Market & Technology Readiness Level

The "Market & Technology Readiness Level" is a method that illustrates the lifecycle of product development from initial idea to commercial product or service. Each level requires other skillsets and knowledge, this method can be useful to identify issues before they arise. The TRL and MRL focus on different aspects:

- 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 shows the TRL scale on the left and the MRL scale on the right.

Figure 1 – On the left side the TRL scale & on the right side the MRL scale (source: TNO tech-transfer[3])

[3] https://www.tno.nl/en/collaboration/tech-transfer/

Figure 2 below shows a combined picture of MRL and TRL and the blue arrow depicts the 'journey' that has to be made from a first scientific result to a usable product or service. See how both MRL and TRL are 0, in the 'Idea phase' and level up to an area in which a product or service becomes usable for an end-user. For a commercial available product or service, the desired TRL would have to be 8 or 9, a level in the scale that indicates an actual usable product or service including support and maintenance. The MRL should be at least 6 or 7, implying a stable business to ensure maintenance and support.

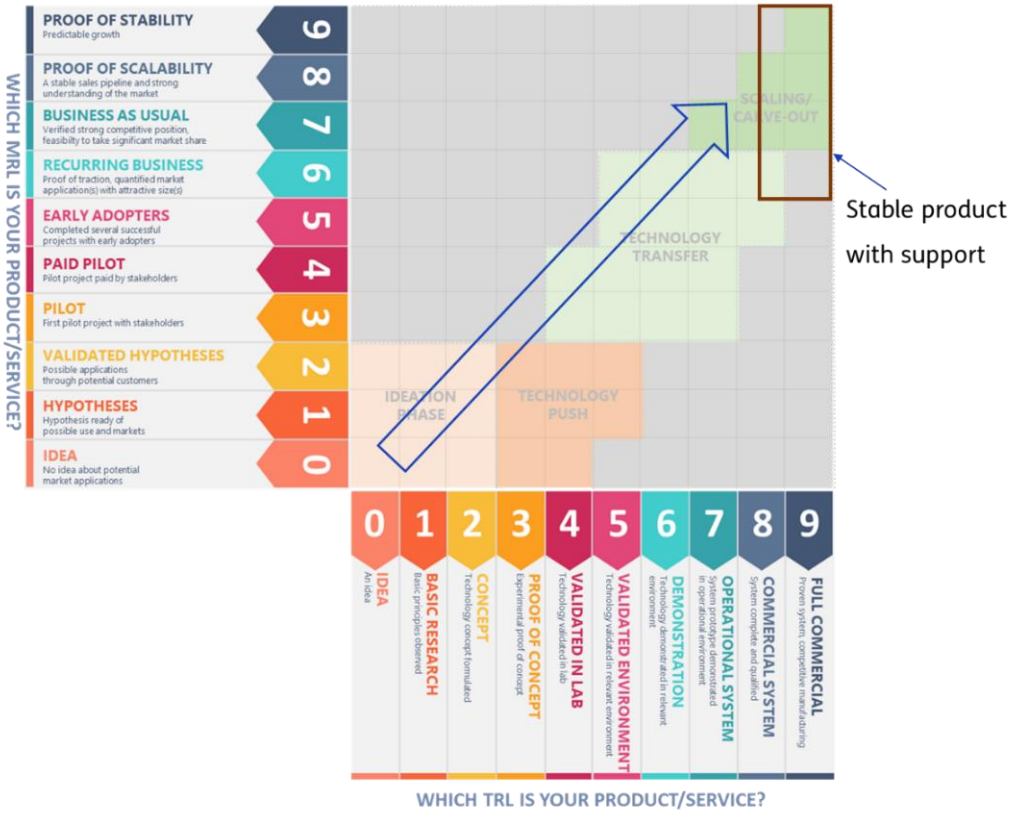

Figure 2 – From idea to product in TRL & MRL

The journey from idea to product or service has many challenges. And to complicate matters further, it often happens that more parties will be involved in different stages of this journey. The different TRL and MRL values require other skillsets and knowledges, we will elaborate more on this in the following chapters. The requirement for different skillsets often leads to a need for hand-overs from one organization to another organization in between the different levels. For example; results of academic research could be handed over to an applied research institute for further applied development; the result of this further development could be handed over to a commercial (start-up) company. During a hand-over, many aspects need to be considered, such as functional and non functional requirements, legal & regulatory topics, IP transfer and costs. The resulting hand-over of an (intermediary) innovation result to a new party is called tech-transfer, see Figure 3 for a visual representation.

Figure 3 - Potential tech transfer/hand-over in innovation projects leading to commercial available products or services

E.g. PCSI (see Appendix C) typically starts projects at TRL level 3-5 (Concept) and MRL level 1-2 (hypothesis) and produces innovation results that are on TRL level 6-7 (demonstrated in operational environment) and MRL level 4 (pilot), so PCSI is part of an innovation chain and there will be several tech-transfers from one party to another.

Tech-transfer of results from one party to another takes much energy; e.g. in the search and selection of receiving parties that deliver that missing skill or technology that brings the higher TRL and MRL levels. And even if a match is found, much time is needed for negotiations on what will be transferred exactly and all the corresponding legal agreements.

Because tech-transfer is hard, it often fails and consequently, good ideas often do not make it into a product or service. The result is disinvestment and less security for end-users.

2.2 Findings from literature

Several literature sources have analysed (cyber security) tech-transfer and its challenges. Schuh and Latz [16] describe technology transfer as “the targeted transfer of technological and technology-related know-how between partners and as a necessity for innovation systems to succeed”. The targeted transfer of technological and technology-related know-how is very difficult to achieve. The problem often occurs from the early adopters to market (TRL 5-8), which is the time that the protype needs to be validated to evolve into a complete operational product. As McKinsey & Company [20] show; many promising technologies – yet uncertain and capital intensive – reach commercialization late or never, and they argue that a change is needed in how technology is transferred from science to industry, especially in European innovation systems.

Below we present a summary of relevant literature and related arguments regarding spin-off success and tech-transfer for highly technical spinoffs.

2.2.1 The right spin off team composition for success

Adesola et al. [17] show that the entrepreneurial capital is a new venture’s most important asset. The experience and knowledge of the entrepreneurs, as well as their network capabilities, are a multiplicative function of entrepreneurial competence and commitment. They mention that the combination of one very committed researcher and an external entrepreneur was the best combination for success for university spinoffs, due to the complexity and required width of knowledge of the different key factors of a spinoff.

Compared to unsuccessful spinoffs, successful spinoffs have “an experienced business coach with complementary skills and experiences who committed one day per week to support the development of the new company. This means that by entering the incubation program they will get access not only to the founding academic team’s network and the existing network of the surrogate entrepreneur, but also to the existing network of the incubator coach”. Partnering with an experienced business entrepreneur gives better insights in market research, market proximity and knowledge. Which leads to even higher startup success rates, if an experienced business entrepreneur is found outside the founders network; such as industry partners according to Sutopo, et al. [6].

2.2.2 Spinoff strategy decisions by mixed entrepreneur/researcher team to prevent bias

Colombo and Piva [19] argue that academic high-tech start-ups exhibit peculiar ‘genetic characteristics’; their strategy often prioritizes further improvement of technological and scientific competencies, instead of being more market demand-oriented. According to Nicolaou & Birley [21] & Halecker and Dotzel [4], this could be in part due to researchers taking active steps to preserve their academic identity when participating in technology transfer activities, by either delegating the business or doing business as well as research activities. This means that the impact of an academic only team might be bigger with highly technical spinoffs, such as deep tech. The academic increased focus on technology and scientific competencies, could harm the commercialization (tech-transfer) process.

2.2.3 Deep tech startup challenge: parallel development of startup and market

Some studies have examined the commercialization of highly technical spinoffs, particularly when the market struggles to grasp the project or its end result. Understanding the project is especially important when the uncertainty of the return of investment is very high, while the iterative nature of the explorative R&D results in high R&D costs required until successful exploitation occurs, noted by Adesola and Datta [17]. This results in unique challenges for deep tech startups, as they often emerge from market niches without existing markets or players, creating an opaque business case with many unknowns, as argued by Schuh et al. [18]. Additionally, deep tech startups aim to disrupt existing markets or create new ones with their innovations, but the actual impact is hard to calculate until adoption occurs. Schuh et al. [18] conclude that deep tech startups and spinoffs “(...) face the challenge of not only developing their organization, but also developing their technology and building a market in parallel.” They often fail because they focus too much on operations and neglect strategic planning and objectives Many deep tech spinoffs deal with major market risk, due to their novel products and technologies, which are not yet embedded in society. During the product development it’s not yet known, how system integrators and end customers will react to these innovations. Therefore, the direct commercial applications of the core technology are not usually immediately evident, reducing investor attraction[4].

Halecker and Dotzel [4] propose an alternative in their deep tech commercialization model. They suggest that tech-transfer activities can be divided into two parts (see Figure 4). The ‘Technology development’ can be handled by the academics on the spin-off team to create a generic building block for the technology. Meanwhile, the entrepreneurs focus on applying this generic building block in the market.

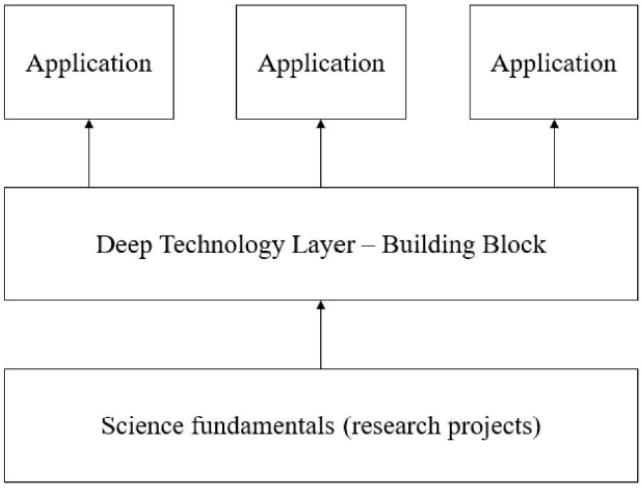

Figure 4 : Framework for deeptech commercialization (Halecker and Dotzel, 2023, p.6)

With this model, they argue that the common lack of entrepreneurial skills, familiarity with industrial use cases and venture capital within the development stage can be circumvented by outsourcing the final development steps and letting the researchers focus on the technology. The outsourcing can be done by transferring the final development steps not only in spinoffs but also through licensing existing or newly founded companies.

2.2.4 Financing Deep tech startups is high cost-high risk

As mentioned, these high-risk, high-cost circumstances limit the enthusiasm of financiers. Additionally, the high risk and cost associated with deep tech startups increase both the time needed to secure financial resources and the overall amount of money required. . Fukugawa [10] suggests that research institutions and universities could increase their financial means to put more effort in research that results in patents. This helps to signal to outside financiers such as venture capitalists how successful their spinoffs and IP is. Venture capital involvement is a positive influence for deep tech startups with the coaching and market connections they provide.

Kashef et al. [22] highlight a paradox for cybersecurity research in their recent work t is a meta-discipline based on cross-sectoral partnerships. They point out a disconnect between ad hoc industry solutions and academic research, which is further complicated by restricted access to cyber systems and data in real-world applications. This limits researchers from comprehending current cyber issues in practical real-life settings impacting both industry and the public sector. As a result, research solutions often become inaccessible or unsuitable for real-world applications. Also, the research solutions are often misaligned with industry's short-term goals of reaching the market with an innovative idea before competitors and immediate market-driven cybersecurity challenges.

Kashef et al. [22] conclude that transition of research spinoffs to industry can be accelerated if industry stakeholders grasp the scientific rigor needed for academic publications, while academic partners consider industry deliverables and need for market connection. A key component to success is academics and industry working together to clearly define the problem instead of only aligning primary outcomes. This includes collecting feedback from potential customers. With this alignment we accelerate knowledge- and tech-transfer and optimize the internal drivers (operational effectiveness) of universities and industry.

2.3 Learnings from practice: barriers

This paragraph highlights the barriers as experienced by the organizations and people that we have interviewed.

2.3.1 Entrepreneurial climate

The entrepreneurial climate for cyber security always follows the movement of digitalization. Cyber security often finds itself at the end of a change or a product cycle, after a technology is implemented in society. This means that security controls are implemented after the product or service is implemented. Because of time pressure, the security controls are implemented with existing security products and services that are readily available on the market. This does not stimulate innovation in cyber security, that requires a more forward looking approach.

Another aspect is that the entrepreneurial climate in the Netherlands focusses on investment in IT businesses that have predictable Return on Investment (ROI) margins; the climate tends to be risk-averse. Companies prefer to offer services with a predictable ROI rather than innovative cyber security services, whose financial outcomes are less predictable. Innovative cyber security products and services are in many cases not a guarantee for positive business cases. The right balance between technical innovation and what customers are willing to pay for security is a challenge. We`ve spoken to several companies and vendors who don't have a structural approach on innovation, but rather rely on an ad-hoc approach.

In the US, we see a different entrepreneurial climate, in which companies (or CISO's) are prepared to try out new things and take some risks. The venture capital scene also embraces risk-taking, creating an ideal environment for an entrepreneurial cybersecurity climate. This mindset naturally fosters innovation.

2.3.2 Market

While the EU is theoretically a single market, in practice, there are significant differences in market conditions and regulations between member states. This fragmentation hinders easy market growth and deters potential investors in innovative products. In contrast, the US operates more like a unified market with relatively uniform regulations across states. This consistency allows for faster market growth, making investments in innovative products and services more profitable. So, it's more attractive for companies to go public, generating capital for new investments. This dynamic is one reason for the investment gap between the US and the EU.

Moreover, in the Netherlands, national security isn't seen as a strong business driver, unlike in countries such as the USA, Israel, the UK, China, Taiwan, and Korea. In these countries, heightened cyber risk awareness likely boosts commercial demand for cyber security products and services, creating a knowledge chain that links academic research to applied innovation, applied innovation to tech-transfer, and tech-transfer to market exploitation and growth. Although the EU has made progress with the gradual introduction of NIS1 and NIS2 requirements, it hasn't yet significantly boosted tech transfer.

2.3.3 Technology oriented versus service oriented companies

The Netherlands does not have a good track record in technology oriented cyber security innovation. The exact reason is unclear, but all other barriers that are mentioned in this paragraph will have influence. There are however, a relatively high number of successful service oriented companies such as Managed Security Providers (MSSPs), and companies offering forensic security and security awareness. Setting up a service oriented company

can be less attractive for investors, because service ideas are generally harder to protect. Consequently there`s little or no well-defined Intellectual Property Right (IPR) to offer value to investors. On the other hand, protecting technology through e.g. a patent takes effort and money. And when other companies challenge the patent it can become even more costly and even turn into lawsuits that need to be managed.

Another aspect to consider is the use of open source resources. Open source software also comes with specific licenses, that can even vary per region. This could complicate matters when launching new products or services built on open source resources.

2.3.4 End-user behaviour

Small and Medium Enterprise (SME) end-users are mostly looking for value for money and do not have substantial budgets for large investments in cyber security products, which hampers innovation and tech transfer.

Large end-users, like banks, telcos, and high-tech industries, have the budgets to spend but often avoid small suppliers or start-ups, even those with innovative ideas. These small vendors typically offer niche products or services. From a supplier management perspective, end-users prefer not to deal with numerous suppliers as it increases complexity and the effort required for third-party management. As a result, they tend to rely on a limited number of large security suppliers, often based outside the Netherlands or even the EU. To stand a chance, a small vendor needs to have an excellent offer that really solves a problem for the end-user that cannot be solved by large suppliers.

Besides, security departments and CISOs usually don't have large budgets. The role of CISO is a relatively new role, and CISO's are often relatively young compared to board members. Explaining the cyber security business case to a board can be difficult; it`s still seen as a cost factor in many cases. This results in difficulties in securing budget, even if security people would like to invest in innovative products and services.

2.3.5 Technology Lock-in

Most end-users make use of a limited set of technologies or technology providers. A famous example is the Microsoft Office suite, that is used by a majority of end-users. These end-users select (security) service providers that fit their technology choices. These (security) service providers often have partnerships with the large technology providers. If a (security) service provider wants to implement innovative ideas, it will (need to) collaborate with the technology provider because the innovation needs to be able to interact with the technology of the specific technology partner.

A start-up that is built around an innovative idea needs to ensure that the resulting products or services are compatible with the large technology providers, because if not, there will be no market for it.

2.3.6 Knowledge and people

To be able to successful innovate on cyber security, the availability of knowledgeable experts is a prerequisite. In the Netherlands, we've seen a rapid increase in cybersecurity courses at all levels. Cyber security academic, higher professional education and secondary vocational education. This is a positive development that should help alleviate the shortage of cyber security experts, which is great news for innovative companies and start-ups.

Despite the growing number of knowledgeable experts, there's still pressure on the labour market. Primarily, people are needed in operational jobs, managing security in e.g. Security Operation Centres. This leads to attractive labour conditions for such jobs and

consequently has the risk of pulling away people from innovation activities. The increasing level of automation in security operation activities could ease some of this pain.

Another factor is the high number of foreign academics being educated and working for Dutch universities. Many of these people will return to their home country making them unavailable for innovation activities in the Netherlands.

And lastly, also foreign companies experience the scarcity in cyber security experts, leading to Dutch experts working abroad and thus not contribute to security innovation in the Netherlands.

2.3.7 Regulations

In recent years we see a rapid increase in EU regulations regarding cyber security matters. It all started with the General Data Protection Regulation (GDPR) for safeguarding privacy, but currently several new regulations are being introduced or have been introduced. The most important ones:

- Network and Information Security Directive 2 (NIS2), that imposes stricter cybersecurity obligations on entities operating in various critical infrastructure sectors, as well as important sectors. It will cover all large and medium-sized companies in these sectors and will tighten rules on risk management, incident reporting, information sharing, and more;
- Cyber Resilience Act (CRA), which imposes cybersecurity requirements for products with digital elements, and bolsters cybersecurity rules to ensure more secure hardware and software products;
- The Digital Operational Resilience Act (DORA), a digital operational resilience framework aimed at financial institutions, such as banks and payment providers. It aims to ensure that these institutions are able to protect against, respond to, and recover from different ICT-related attacks and threats.

Regulations can be a blessing for CISO's when requesting budgets from their boards to invest in cyber security measures. With regulatory obligations in place this will become easier.

But regulations also have a downside, especially for innovation. One example that was brought forward by one of the interviewees:

Example of regulatory barrier for innovation

A company wanted to introduce a new service in NL. This service already was introduced in the UK (outside EU) and it used technology from another country outside the EU. Technically, implementing the service in the Netherlands was easy. However, since the UK is outside the EU and the technology also came outside the EU, it took a year of legal work before the service could be introduced.

Besides that it takes up valuable lead time, complying to regulations also requires knowledge that is scarce; when in an innovation project or in a start-up, proving compliance to regulations gobbles up valuable time that also is needed to improve the product or service and conquer the market.

Also, EU regulations will need to be elaborated in national legislation per country. This again could lead to differences in legislation per country, which could slow down market introduction of new and innovative products and services.

2.3.8 Scalability

New innovative products or services are usually piloted and tested at (potential) customer environments, TRL 6-7 and MRL 4-5 (see section 2.1). The challenge is to scale up a

product or service in such a way that most customers can use the same version. Creating customized versions for each new customer makes market introduction more complex and time-consuming. The technology lock-in as described in section 2.3.5 plays a role here, but also the question how easy a product or service can be integrated in an end-user environment.

2.3.9 Take-over of successful companies

When an innovative security product or service becomes successful and gains high traction and market share, it becomes an attractive target for large (security) companies. These companies have the means to buy such (start-up) companies and add the products, services and customer base to their own existing business. This is an interesting model for those companies, because the success is already there and they do not have to do risky investments in new start-ups or product innovation, of which success is not guaranteed upfront. As indicated in section 0, the available capital for take-overs is higher in countries outside the EU. This increases the risk that ownership, Intellectual Property Right (IPR) and technology will move to outside the EU, making the EU dependent of other countries and regions. What makes matters worse is that in some cases these new (start-up) companies have been supported by EU and Dutch subsidies, which are aimed to build a sovereign EU industry.

2.3.10 Subsidies

Many sources of subsidies are available in the EU and the Netherlands to stimulate (security) innovation. Some of the most important are:

- Horizon Europe, EU's key funding programme for research and innovation. The indicative funding amount for Horizon Europe for the period 2021-2027 is EUR 93.5 billion.
- The Digital Europe Programme, financial contribution from the Union under Specific Objective 3. Topics include strengthening the SOC Ecosystem, National SOCs and developments and deployment of advance key technologies
- The CS4the Netherlands programme for cybersecurity-innovation, that gives a substantial boost to cybersecurity-related knowledge and innovation in the Netherlands, already surpassing 20 million euro for subsidies in 2023. It fosters expertise and innovation through partnerships between industry and research in calls for proposals.

In the Netherlands, the Netherlands Enterprise Agency[4], part of the ministry of Economic Affairs, plays an important role in supporting companies to acquire subsidies.

While subsidies are beneficial for promoting innovation, they also have some pitfalls:

- Small companies are not always aware of the potential sources and benefits of cyber security subsidies. They need to deal with enormous amounts of information on various aspects and information on potential subsidies is sometimes scattered and/or the final benefits compared to the conditions are difficult to assess;
- The large research programs (such as Horizon Europe) insufficiently succeed in letting Small and Medium Enterprise (SME) Companies profit from these innovation funds; most funding is received by large enterprises. Dutch reality of the cyber security landscape is that it mostly consists of SMEs with less than 50 FTE;

[4] https://english.rvo.nl/

- To prevent market disturbance, subsidies come with conditions. These are conditions on the way of working (e.g. building consortia with a minimal number of partners), IPR of the result (e.g. preferring open source solutions, making available IPR to third parties). These conditions could be in the way of entrepreneurship and this is why companies sometimes deliberately choose to avoid using subsidies.

Concluding, although subsidies are a good instrument in stimulating innovation, they are not the ideal solution in all situations. This leads to less effective result of the subsidies and less budget available to companies that could benefit, which could result in delays in product launch, less functionality and market success.

2.3.11 Competition in commercial bids

When a large end-user intends to acquire a new product or service, it is good practice to ask the suppliers that offer such products or services in the market to make an offer. This process is called 'Request For Proposal (RFP)'. When the expected amount for the procurement is above a certain financial threshold, publishing a RFP is mandatory for public institutions in the EU. In practice, an end-user defines a RFP in relative isolation, taking only its own demand into account and often insufficiently takes into consideration the actual market conditions and product or service maturity in the market. This frequently leads to complex RFP processes with long lead times.

Sometimes, in case of complex products or services or when the request is not clearly defined, the RFP can be preceded by a Request For Information (RFI). The RFI is intended to further detail the actual request (with support of the answers provided by suppliers) to be put in a RFP and could also help in selecting the suppliers that will receive an RFP.

Answering a RFP is usually an elaborate and time consuming process for a supplier. Not only needs to be exactly defined what will be delivered both functionally and non-functionally, but also the commercial offer needs to be detailed; the commercial conditions need to be such that they are competitive compared to other suppliers (to win the RFP), but at the same time still provide a profit for the supplier.

Needless to say that responding to RFPs is a necessity for suppliers that want to keep and expand market share. But especially for start-ups with innovative products and services, this is a big hurdle to overcome.

2.4 Learnings from practice: solutions

Transforming good ideas and innovative results into products and services that can be used in practice remains to be a difficult journey. As described in section 2.1 there can be several points in the journey towards a market ready product or service in which hand-overs between different parties are happening: we call this tech transfer. There appears to be a 'Valley of Death' specifically between TRL 6 and 8 and MRL 3 and 5, comparable to the tech transfer gap as experienced in PCSI (see also section 2.1).

In this section we summarize learnings as gathered in interviews and workshops with relevant stakeholders from the cyber security innovation community, that can enhance the chance on successful exploitation of security innovation and overcome this Valley of Death.

2.4.1 Entrepreneurial climate

For an improved entrepreneurial cyber security climate, we need to embed security during the whole product cycle: security by design. The new EU legislation such as NIS2 and the Cyber Resilience Act (CRA) decree that all operational technology and products must be

cyber security safe throughout their life cycle. The long term lifecycle cyber security view isn`t optional anymore. The new interest and mandatory requirements will increase demand in the Dutch and EU cyber security market and entrepreneurial climate. This will increase the amount of cyber security companies as well as their expertise.

2.4.2 Demand and end-user driven

In practice, we see that start-ups that have success mostly have founders that have worked in the industry for a while and are familiar with the issues that CISO's have to face in their daily jobs. So a successful start-up usually is user-demand driven and not technology driven. End-user involvement during development is essential for acceptance of innovations and successful exploitation or tech-transfer. Engaging end-users at appropriate stages in a project ensures user-centricity without affecting the development timeline or innovation process. It helps to have one or more committed customers that have the intention to make use of the final product or service.

This attitude starts at the research level, at TRL 1-3. Research proposals should be judged not only on scientific quality, which of course remains the most important factor, but also on their potential to be developed into market ready products and solutions.

2.4.3 Clear business case

The business case is very important to balance the costs and the benefits. It should clearly outline and demonstrate measurable, tangible benefits that the end-users will gain when using the product or service. Also it should define costs versus expected turnover and profit. For start-ups it is usual that the first period will not be profitable because it is needed to build up the market and customer base.

2.4.4 Investors and support

Investors are needed to finance product development and market introduction, especially for start-ups. Investors should at the latest be involved at TREL 6 when there's a functioning prototype and clear understanding of market potential. For investors to invest, it's crucial that the innovation addresses a tangible need with a defined target market eager to buy the product or service.

Ideally, investors are involved that are willing to invest both financially and strategically, which serves as a commitment to the innovation's implementation. Investors could e.g. provide advice on market approach, availability of subsidies or connect the start-up to interesting parties.

Support could also be given by e.g. the government or branch organisations, to stimulate the innovation climate. This support could be financial in nature, but also in the form of hands-on support, such as introducing a tech-transfer coach who assists in the transition from innovation result to usable product. Furthermore, providing templates, methods and tools that can aid in specifying technology transfer requirements. In NL, RVO and dcypher fulfil such roles.

When developing new products or services, it is important to know 'what is already out there'. Of course there are many information sources, but some of this information is biassed (e.g. communication for commercial purposes) and it is difficult to get a systematic overview of the technology landscape and ongoing innovation activities. It would be good to make unbiassed and timely information on the technology landscape easily available for innovative projects and start-ups by e.g. (a collaboration of) the government, branch organizations or knowledge institutes. An example could be the introduction of a tech-transfer radar that can provide a comprehensive overview of ongoing innovation activities, market trends, and emerging opportunities. Another example could be to facilitate industry-wide collaboration and knowledge exchange

sessions between innovation projects and other stakeholders, such as investors and branch organisations in order to exchange ideas and sharing expertise.

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).

2.4.5 Staffing

When developing new and innovative technology, the chances of bringing such innovations to the market should be assesses as early as possible. When the decision is taken that the technology could be successfully introduced as commercial product or service, the focus should be on this end-result. As described in section 2.2.2 and 2.2.3, the team that is working towards exploitation should be a combination of technical researchers and entrepreneurs, so progress is made on the technical development and market readiness in parallel. We could describe the entrepreneurial team member as a 'business savvy co-worker' that looks to a project from business perspective. While the main focus should be on achieving the end result, the entrepreneurial team member should also maintain an external perspective. This member should not hesitate to call potential customers, such as CISOs, to verify the assumptions being made in the project.

The scarcity of cyber security experts could be eased by e.g. off-shoring certain activities, hiring experts from foreign countries or educate people on the job. The government should play a role in increasing the cyber security workforce; this could be done by prioritizing relevant education and making available more budgets for education. But also (temporarily) lowering barriers for experts from foreign countries.

2.4.6 Tech transfer

Preferably in an early stage, it should be clear which hand-overs are needed and what conditions and information are required to safeguard a smooth hand-over, see also section 2.1. Defining a number of SMART KPI indicators for successful hand-over may help evaluating points of continuous improvement these efforts.

To overcome the Valley of Death between TRL 6 and 8 and MRL 3 and 5, it is essential to involve in an early stage at least one committed party (e.g. spin-off, foundation, OS community, etc.) willing to maintain and exploit the results (and eventually support the end-users).

2.4.7 Intellectual Property Right

Protecting Intellectual Property Right is an important aspect of security innovation.

It has several benefits[5]:

- The one that has protected the intellectual property is the only entity with the right to use or reproduce it. Others cannot copy or reproduce it without permission;
- When an innovation in a product is protected, the quality of the product is guaranteed and its origin is clear. This can be an advantage for business, because customers may prefer to buy a product that has passed more restrictive checks (a controlled good);
- Money can be earned not only through direct use of IP, but also indirectly through licensing contracts. This is when a licensor, the owner or representative of

[5] Source: https://europa.eu/youreurope/business/running-business/intellectual-property/rights/index_en.htm

intellectual property, grants a license to a licensee (e.g. another company) to use the IP protected subject matter for a certain period of time;
- Owning a patent or a trade mark can increase the market value and make it easier for a business to find investors or other funding opportunities.

There are several types of IPR protection, some need formal registration (such as trademarks (protects a trade name, company logo, brand or product name), patents (protect a technical innovation), design rights (protect a design, drawing or model) and others will be granted automatically but may need registration, such as copyright (protects e.g. software, photos, websites), trade name right (protects a trade name) and database right (protects against the re-using of data in databases).

It is always a good idea to assess which assets are important for the business case and which assets need active protection and registration. And also be aware which assets have automatic protection that cannot be breached by others.

2.4.8 Know your market

Many stakeholders' emphasized the need to establish a strong connection with the cybersecurity market for projects (or activities) that aim for commercial exploitation. This involves understanding the needs and dynamics of the market, establishing a presence within industry circles, and fostering relationships with key stakeholders who can successfully drive the entry and the growth of innovative results. Thorough market research is essential to gain a complete understanding of the market environment and to serve as the foundation for a market and technology transfer strategy.

Involving a marketing professional in projects aimed at commercial exploitation would be wise. Their expertise in campaign management, digital marketing, and sales enablement can drive innovation uptake within the right market(s) and sustain the market growth of results afterwards.

2.4.9 Create the market

Governments on both EU and country level are a large customer for security products and services and they tend to consider cyber security as a crucial topic, because they need to protect many assets an interests and also need to set an example for other end-users. These governments can stimulate innovative products and services by considering buying products that result from innovation into account when purchasing new products and services; e.g. by preferring products and services from innovative EU-based suppliers. This in turn can provide credibility to these start-ups, enabling them to acquire customers in other domains. This would also help in decreasing the overwhelming dependency the Netherlands has accrued towards specific IT-automation products and/or cloud solutions often belonging to foreign multinationals.

2.4.10 Pre-competitive collaboration

Collaboration is a powerful way to avoid waste of scarce resources and inefficiencies. At the end of the day, (start-up) companies need to sell products and will be each other's competitors. Despite their individual goals, they collectively contribute to enhancing the security of Dutch society, creating a shared interest. Collaboration and the exchange of ideas and information are particularly beneficial during the pre-competitive phase when products are being developed. Below some suggestions to increase collaboration:

- Stimulate and facilitate cyber security incubator communities in which start-ups jointly work on innovation and exchange information and ideas. Potential investors can also be introduced to these incubator communities;

- Stimulate and facilitate innovation collaboration programs in which suppliers, start-ups and end-users collaboratively work on applied innovation (between TRL 4 and 6 and MRL 2 and 4). This is effective, user demand can be clearly articulated and new innovative products can be evaluated using real data of end-users. PCSI is an example of such a collaboration and is already active since 2014 (formerly known as the Shared Research Program Cybersecurity until 2020);
- Foster the industry communities and knowledge platforms such as established by the Digital Trust Center, Amsec, HSD, Connect2Trust;
- Try to stimulate end-users that do not have exact requirements available when they want to purchase new products or services to use the RFI instrument instead of the RFP instrument. And if possible, make it an open RFI. This enables the use of the power of the market to exchange knowledge and collaboratively build up (pre-competitive) knowledge. In the end, each party involved will come out stronger and with an increased knowledge level.

2.4.11 Open source development

Delivering a product or service in an open source model could be attractive for innovation projects or start-ups. The decision to open-source specific innovations requires a strategic approach with long-term consideration. Factors such as which parts of the software stack to open-source, licensing choices, adherence to code quality practices, repository maintenance responsibilities, and monetization strategies need careful planning. Some suggestions to consider in this respect:

- To ensure long-term success for open source projects, the innovation could be transferred to organizations with experience in managing open source initiatives;
- Ensuring code quality in projects that will publish open source code is of high importance. When code quality in lower TRL levels is at par with what is required at TRL 8/9, it will improve the chances of successful use and community uptake of open source projects;
- Making decisions regarding coding standards, standard APIs, security requirements, testing procedures, documentation practices, and community guidelines early in the development process is essential. Early decision-making significantly increases the likelihood that subsequent code contributions will be consistent, secure, well-documented, and easily adoptable by targeted open source communities;
- Identifying and involving open source communities early in the development process can significantly improve the success rate of exploitation. To ensure adoption by these communities, a clear and compelling value proposition for each project or innovation should be articulated;
- Establishing a platform for non-profit start-ups that are financed through cross-subsidization from the profits of other businesses or activities. Instead of selling software licenses, these start-ups provide mentoring services around open source software. This idea emphasizes "open source stewardship" as a responsibility for technology companies.

Finally, managing intellectual property rights in an open source context requires finding a balance between flexibility for users and maintainers while preserving ample opportunities for commercial entities to build on the innovations. This can be achieved by carefully considering licensing terms and other IP strategies and safeguarding involved partners' interests, ensuring a smooth exploitation without surprises for any involved parties.

2.4.12 EU sovereignty

It is difficult to avoid the take-over of successful companies or start-ups by foreign large companies or investors. One opportunity to prevent these take-overs in the Netherlands is

the law that is called ‘Wet veiligheidstoets investeringen, fusies en overnames (Vifo)’. It came into effect on June 1st 2023 and it introduces a safety check for investments, mergers and take-overs that could be a risk for the Dutch national security. Needless to say that this applies only to a limited number of potential take-overs and should be used with care. It could seriously disturb the business case of such a company, the company will be less attractive to investors and the market potential might not be optimally exploited.

3 Conclusions & recommendations

3.1 Conclusions

The general opinion is that the Dutch cyber security ecosystem may not be ranked top of the world, but it is not doing badly in comparison to other regions. The Netherlands has a good knowledge base and educational cyber security environment, its government is relatively cyber-mature and active on cyber security, Dutch investigation services are operating on a high level and are successful and the Netherlands has quite a few companies that are active in the cyber security field. However, transforming good ideas and innovative results into practical products and services remains to be a difficult journey. Not many start-ups have originated from technology developed at knowledge institutes or universities. While a single party, such as a group of researchers, can develop a product or service from an idea at TRL 1 to a commercial product, this journey already is hard and has many challenges. Usually, multiple parties are involved during the journey from idea to product or and there`s a need for handovers; which result in tech-transfer. There is a particularly known gap of tech transfer, aptly called the 'Valley of Death' between TRL 6 and 8 and MRL 3 and 5 (see also section 2.1).

We have identified a number of reasons for this:

- The cybersecurity entrepreneurial climate in the Netherlands is not very positive because there is not yet a 'security-by-design' attitude, cyber security is seen as an unpredictable Return on Investment and financing cyber security start-ups is high-cost high-risk;
- The EU market is scattered because of differences in market and regulation between countries, and in the Netherlands, national security is not a strong business drive. This makes it hard to define a positive business case;
- the Netherlands does have a relatively high number of successful service oriented companies such as Managed Security (MSSPs), and companies offering forensic security and security awareness. But there are not many security technology providers;
- End user behaviour makes it hard for innovative start-ups to be successful; SMEs have limited budgets and large enterprises prefer the stability and track record of large suppliers (which are frequently not the Netherlands-based);
- Most end-users make use of a limited set of technologies or technology providers, which forces suppliers and start-ups to adapt their innovative products to these technologies;
- The scarcity of cyber security experts on the market makes it hard ensure quality and lead times of innovative development;
- Regulations on the one hand stimulate investments in cyber security but on the other hand can slow done innovation because of additional implementation effort and differences in national legislation, even within the EU;
- Scaling up from a successful first-customer launch without creating specials of products and services for each new customer is a challenge;
- When (start-up) companies become successful, they are easily taken over by large foreign companies, which results in IPR and technology moving to outside the EU, making the EU dependent of other countries and regions;
- There are many subsidies available, but they come with conditions and are not specifically suited or hard to find for SME's;
- Time spent on replying on RFPs drains resources and time form (start-up) companies
- It is a challenge for start-ups to develop a new product or service and develop the market in parallel.

3.2 Recommendations

Based on the findings in this report, we have formulated a number of recommendations, specific for the Netherlands and EU government, for end-users and finally for security suppliers, security innovation projects and start-ups, to enhance the chances on successful exploitation of security innovation results.

The Netherlands and EU Government

- Advocate security-by-design as a default approach, so all (innovative) operational technology and products are secure when they are introduced. This is also triggered by the mandatory requirements of regulation that put more focus on security by design and will increase demand in the Dutch and EU cyber security market and entrepreneurial climate;
- Intensify the support that is provided to innovation projects to stimulate the innovation climate, also from branch organizations. Put more focus on cyber security innovation support. Support could be financial in nature, but also in the form of hands-on support, such as introducing a security tech-transfer coach who assists in the transition from innovation result to usable product;
- Make unbiassed and timely information on the technology landscape easily available for innovative projects and start-ups. In a technology landscape, aspects are made available such as state of the art, technology trends, innovation initiatives in the Netherlands and globally. This should be a shared responsibility of the Dutch government, knowledge institutes and branch organizations;
- Play a stronger role in enlarging and strengthening the cyber security workforce; this could be done by prioritizing relevant education and making available more budgets for education. Additionally, barriers for hiring experts from foreign countries could be (temporarily) lowered;
- Facilitate and stimulate cyber security incubator communities in which start-ups jointly work on innovation and exchange information and ideas. Potential investors can also be introduced to these incubator communities;
- Increase the effort that is put in facilitating innovation collaboration programs in which suppliers, start-ups and end-users collaboratively work on applied innovation (between TRL 4 and 6 and MRL 2 and 4);
- Keep a sharp eye on the number of take-overs of successful cyber security companies or start-ups by foreign large companies or investors. Depending on the context, such take-overs could be harmless or even beneficial, but in some cases these take-overs might be a threat to the Dutch and EU sovereignty.

End-users (including governments)

- Embrace an innovative, forward looking mindset in which there is room for experiments and failure. This will support end-users in being prepared for new threats, upcoming regulations and other changes;
- Improve the availability of innovative products and services by taking innovation prowess into account when choosing a vendor to purchase new products and services; e.g. by preferring products and services from innovative EU-based suppliers. This in turn can provide credibility to these start-ups, enabling them to acquire customers in other domains;
- Require products and services that are purchased to be secure by design, so products and services are secure when the end-user starts using them;
- Make more use of collaborative knowledge for pre-competitive activities. End-users that do not have exact requirements available when they want to purchase new security products or services could make more use of knowledge platforms (e.g.

established by the Digital Trust Center, Amsec, HSD). End-users could also launch an open Request For Information (RFI), in which potential suppliers can support the end-user in further defining the end-user need.

Security suppliers, security innovation projects and start-ups

- Embrace security-by-design as a default approach, so products and services are secure when they are introduced to the market;
- Be demand-driven and end-user driven and not technology-driven, starting from the lower TRL levels. Involve end-users in an early stage of development whenever possible;
- Ensure that the business case for innovation has measurable tangible benefits that the end-users will profit from when using the product or service;
- Involve investors that are willing to invest both financially and strategically, offering advice and support;
- Ensure that the team that is working towards exploitation is a combination of technical researchers and entrepreneurs, so progress is made on the technical development and market readiness in parallel. It would be wise involving a marketeer role (for campaign management, digital marketing, and sales enablement) in projects (or activities) that aim for commercial exploitation;
- Be creative in managing the scarcity of cyber security experts that are needed for innovation activities (technical security expertise, but also e.g. security risk, human factor security, security governance). The scarcity could be eased by e.g. off-shoring certain activities, hiring experts from foreign countries or educate people on the job;
- Be aware of which hand-overs are needed in tech transfer(s) during an innovation project and what conditions and information are required to safeguard a smooth hand-over;
- To overcome the Valley of Death between TRL 6-8 and MRL 3-5, involve at least one committed party (e.g. spin-off, foundation, OS community, etc.), willing to maintain and exploit the results and eventually support the end-user, in the early stages of innovation;
- Assess which assets are important for the business case and which assets need active (IPR) protection and registration;
- Take into account relevant aspects in a decision to open-source specific innovations. These aspects could include: which parts of the software stack to open-source, choice of license, adherence to code quality practices, repository maintenance responsibilities, and monetization strategies.

We conclude that bridging the tech transfer gap(s) remains challenging. Successful navigation of these gaps in the Netherlands requires cooperation between different parties and a careful assessment of needs at each handover, with a focus on customer needs. We think that the recommendations above can help in managing the innovation and tech transfer challenges.

References

Nr	Title	Author	Year	Source
1	De economische kansen van de cybersecuritysector	Dialogic (in opdracht van min. EZK)	2023	https://dialogic.nl/wp-content/uploads/2023/06/economische-kansen-van-de-cybersecuritysector-7.pdf
2	Technology transfer from national/federal labs and public research institutes: Managerial and policy implications	Donald Siegel, Marcel L.A.M. Bogers, P. Devereaux Jennings, Lan Xue	2023	Elsevier Research Policy Volume 52, Issue 1, January 2023, 104646. https://www.sciencedirect.com/science/article/pii/S0048733322001676
3	The Who, Why and How of Spin-offs	Dahl, Michael S.; Sorenson, Olav	2012	In Academy of Management Annual Meeting 2012 Academy of Management. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2089495
4	From Building Block to Application: A Deep Tech Commercialization Framework	Halecker and Dotzel	2023	https://www.proquest.com/docview/2840810979?pq-origsite=gscholar&fromopenview=true
5	TNO tech-transfer programma jaarrapportage 2022	TNO Tech-transfer	2022	TNO internal
6	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. https://www.mdpi.com/2199-8531/5/4/95
7	Technology transfer and defence sector dynamics: the case of the Netherlands	Mustafa Ali Sezal & Francesco Giumelli	2022	EUROPEAN SECURITY 2022, VOL. 31, NO. 4, 558–575 https://doi.org/10.1080/09662839.2022.2028277
8	Technology Transfer: From the Research Bench to Commercialization. Part 2: The Commercialization Process	Gail A. Van Norman, Roï Eisenkot	2017	JACC : Basic to Translational Science, Volume 2, Issue 2 , pages : 197-208. https://www.sciencedirect.com/science/article/pii/S2452302X17300529
9	open source Archetypes: A framework For Purposeful open source	Mozilla blog	2018	https://blog.mozilla.org/wp-content/uploads/2018/05/MZOTS_OS_Archetypes_report_ext_scr.pdf
10	Effects of the quality of science and innovation on venture financing: evidence from university spinoffs in Japan	Nobuya Fukugawa	2005	Applied Economics Letters. https://doi.org/10.1080/13504851.2022.2094319

11	open source references	From interview Karim Al Assal		https://www.tno.nl/os https://open-source-strategy.gitlab.tsn.tno.nl/general/commercial-opportunities/ https://choosealicense.com/
12	Onderzoek naar de impact van R&D&I in het cybersecurity domein	Marcel de Heide et al. (TNO, Dialogic, SEO))		https://www.seo.nl/wp-content/uploads/2023/11/2023-120_TNO-2023-R11836.pdf
13	Crossing the "Valley of Death": Transitioning Cybersecurity Research into Practice	Maughan, Balenson, Lindqvist, Tudor	2013	https://ieeexplore.ieee.org/abstract/document/6493323
14	Crossing the Great Divide: From Research to Market	Terry V. Benzel et.al.	2013	https://ieeexplore.ieee.org/abstract/document/6493324
15	Crossing the Great Divide: Transferring Security Technology from Research to the Market	T. V. Benzel and S. Lipner	2013	https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6493322
16	Concept for the Identification of Governmental Needs for Actions within the Technology Transfer of Deep Tech	G. Schuh, T. Latz	2022	In 2022 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) (pp. 1015-1020). IEEE. https://ieeexplore.ieee.org/document/9989824
17	Spin-Off Strategy and Technology Transfer Office: Cases in Sweden	S. Adesola, S. Datta	2020	https://doi.org/10.1007/978-3-030-48013-4_5
18	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 https://d-nb.info/1253580243/34
19	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. https://www.sciencedirect.com/science/article/pii/S0048733311001673
20	Deutschland 2030: Kreative Erneuerung	McKinsey & Company	2021	https://www.mckinsey.de/publikationen/deutschland2030-kreative-erneuerung
21	Academic Networks in a Trichotomous Categorization of University Spinouts	Nicolaou, N. and S. Birley	2003	Journal of Business Venturing 18, 333–359. https://www.sciencedirect.com/science/article/pii/S0883902602001180
22	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. https://rshare.library.torontomu.ca/articles/preprint/Bridging_the_Bubbles_Connecting_Academia_and_Industry_in_

				Cybersecurity_Research/24132645
23	PCSI tech-transfer – Improving the applicability of PCSI security innovation results	Reinder Wolthuis, Marth Breure, Ruggero Montalto	2024	TNO report number TNO 2023 R11589 https://publications.tno.nl/publication/34642234/1rUnk7/TNO-2023-R11589.pdf
24	Security Innovation stories: 20 koplopers over innovatie in het cybersecuritydomein	Bram de Bruijn, Frank van Summeren	2024	https://www.securityinnovationstories.com/boek/

Appendix A Interviewees

The table below shows the people that were additionally interviewed for this report. During the first part of the project, a number of interviews and workshops were conducted as shown in appendix A of [23].

Name	Organisation	Role of Organisation	Role description
Reinout van der Meulen	TIIN Capital	(Cyber security) investment company	Provide promising ideas/startups with financial means to grow
Eddy Boot	dcypher	Cybersecurity cooperation platform for research and innovation in the Netherlands	Bring organizations together in education, research and innovation for the development of concrete applications
Floris Dankaart	Fox-IT	MSSP	Offer cyber security services to customers
Liesbeth Holterman	Cyberveilig Nederland	Branche organization	Represent interests of collective cyber security companies in the Netherlands
Martijn Neef	Ministry of Economic Affairs	Dutch Ministry	Create an excellent entrepreneurial business climate, and encourage cooperation between research institutes and businesses

Appendix B Glossary

Glossary

CI/CD	Continuous Integration/Continuous Development
CISO	Chief Information Security Officer
CRA	Cyber Resilience Act
DORA	Digital Operational Resilience Act
EU	European Union
EZ	Economische Zaken (Ministry of Economic Affairs)
GDPR	General Data Protection Regulation
IPR	Intellectual Property Right
ICT	Information & Communication Technology
IT	Information Technology
KPI	Key Performance Indicator
MRL	Market Readiness Level
MSSP	Managed Security Service Provider
NIS (1 and2)	Network and Information Security Directive (1 and 2)
OS	Open source
PCSI	Partnership for cyber security Innovation
PoC	Proof of Concept
RFI	Request for Information
RFP	Request for Proposal
ROI	Return on Investment
RVO	Rijksdienst voor Ondernemend Nederland (Netherlands Enterprise Agency)
SMART	Specific, Measurable, Assignable, Realistic, and Time-bound
SME	Small and Medium Enterprise
SOC	Security Operations Center
TNO	Nederlandse organisatie voor toegepast-natuurwetenschappelijk onderzoek
TRL	Technology Readiness Level
UK	United Kingdom
US	United States
VC	Venture Capitalist

Appendix C The PCSI

PCSI

Project team – PCSI is a real collaborative innovation effort. In the project team, all core partners can participate with their experts; experts are expected to spend an average of 2-4 hours weekly on project contributions. A project team always has a TNO project lead and there should be experts from at least two non-TNO partners in the team.

Liaison Partner - Liaison partners are organizations that are strongly interested in both learning from and contributing to current and future cyber security innovations being worked on within PCSI. Liaison Partners are organizations that do not have the resources or scale to become a core partner or are organizations offering commercial security services (and therefore cannot become a core partner). All liaison Partners are invited at least once a year for a PCSI Liaison Partners' event. By acceptance of PCSI coordinators (and under continuous scrutiny of the independent TNO Project leads) Liaison Partners can be invited to join specific projects in which their expertise can mutually beneficial combine with the expertise of PCSI core partners.

PCSI innovation process

The PCSI innovation process is a continuous cycle of four months; each four months, new projects will start and running projects are assessed on several aspects after which they will receive a Go or No-go for the next cycle. The process currently has four cycles: Explore, PoC, Pilot and Exploit.

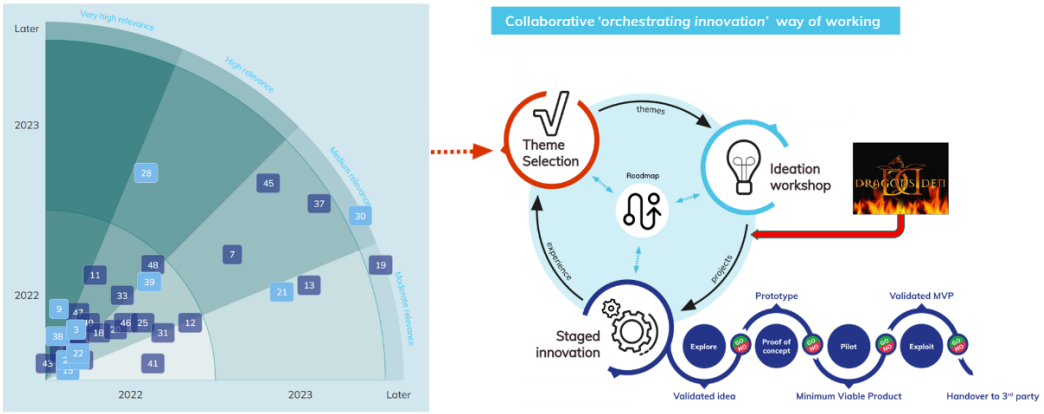

Figure 5: The PCSI innovation process

Security Radar - The security radar contains relevant security themes for the partners in PCSI, actual themes but also looking into the future. It will assess the relevance of those (future) security themes for the participating partners and Dutch society. Themes include emerging threats, but also security-relevant developments on technical, organizational society level. A continuous activity in PCSI is dedicated to keep the security radar up-to-date.

Theme selection - The Steering Committee will select each four months the themes that are addressed in the coming period. Input for this selection is the Security radar. The number of themes varies between one and three, depending on the number of projects that are already running.

Ideation Day – Ideation on the selected themes is organized as a face-to-face full day event; in the morning, Ideation workshops are organized in parallel, early afternoon pitches are prepared and late afternoon the project ides are pitched before the Dragons, which then will decide which pitch is allowed to continue as a project

- Ideation workshop- An Ideation workshop is organized for each of the selected themes from the theme selection step. We apply a specific brainstorming format to organize this effectively and it is facilitated by an Ideation expert. All partners are invited to delegate their relevant experts on the theme to the Ideation session. Typically, several project ideas are generated in each Ideation session, but eventually one project idea is selected. The experts that staffed the Ideation session will get the opportunity to work on it in the project.
- Dragon's Den - The selected project idea(s) from the Ideation session(s) are pitched before a Dragon's Den (PCSI steering committee). They decide whether a project pitch actually is rewarded and can enter the short cyclic innovation process.

Staged innovation

- Presentation Day - Each three months, a PCSI Program presentation day is organized, during which the project results for the concluded phase are presented and discussed and the Go/No-Go decision is made for each project to enter the next phase. A project that receives a 'Go' to enter the next phase will only be provided with budget and means for this next phase, At the end of the next phase, the project again will have a Go/No-Go decision.
- Explore phase - The goal of the explore phase is the Explore the project idea further. An assessment will be done on the Stat-of the-Art of the selected topic and the anticipated end result of the project will be further defined. At the ned of the Explore phase there should be either a plan to build a PoC or a proposal to stop the project (e.g. because there already are products on the market that fulfil the innovation need).
- PoC phase – In the PoC phase, a proof of concept will be built. This can be a technical tool, a methodology, a process or even a new role description. At the end of the PoC phase the PoC should be ready and a plan to conduct a pilot with the PoC must be available. Alternatively, the project team could also propose to stop the project because no realistic pilot can be conducted.
- Pilot phase – In the pilot phase, the PoC is tested in a realistic (operational) environment at one of PCSI core partners. At the end of the PoC phase, a pilot evaluation must be available and also a proposal for Exploit phase activities. Alternatively, the project team could also propose to stop the project because the pilot results proved that continuing with Exploitation is not a good idea.
- Exploit phase – In the Exploit phase, a plan is made to ensure that the result is not ending up in a drawer. Exploitation can have several forms, such as transfer to a security vendor, publishing as open source, publishing articles or whitepapers etc. The final result and follow-up plans are presented to the Steering Committee for approval.