REPORT PHASE 2

Call reference: 241018

Study on the creation of an ecosystem for defence and dual-use start-ups / Kaitsevaldkonna ja kahese kasutusega iduettevõtluse ökosüsteemi loomise uuring

Uuringu tellis Kaitseministeerium programmi „Valdkondliku teadus- ja arendustegevuse tugevdamine” (RITA) raames. Projekti rahastatakse RITA tegevuse 2 raames Euroopa Regionaalarengu Fondist ja Kaitseministeeriumi eelarvest.

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

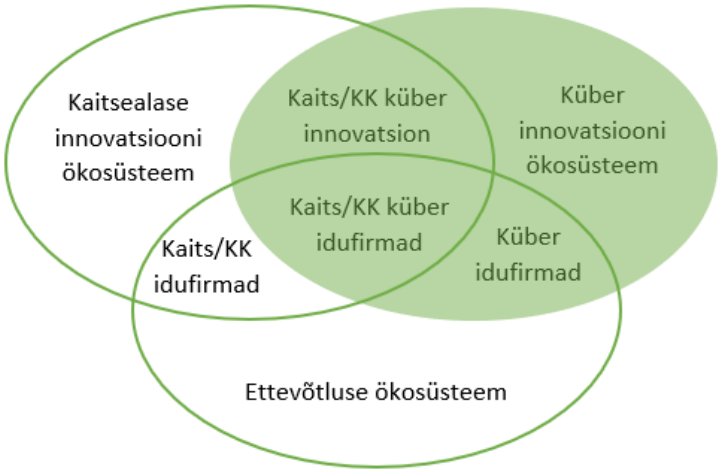
Juuni, 2022

Table of Contents

Kokkuvõte

See on pakkumuse nr 241018 raames algatatud projekti teine etap. Raporti 1. faasi võib tõlgendada erinevalt ja see keskendub kahese kasutusega kaitse- ja julgeoleku iduettevõtete maailma edulugudele. Analüüsiti selle vertikaali idufirmasid üle maailma, et teha kindlaks, milliseid ökosüsteeme võiks Eesti jäljendada, milliseid omadusi arendada ja milliseid omadusi vältida. Sealse uuringu põhjal tuvastati kaks ökosüsteemi Ühendkuningriigis ja Singapuris. Need olid Eesti vajadustele kõige lähemal ning sellised ökosüsteemid nagu USA ja Iisrael jäid nende raharikka positsiooni tõttu kõrvale. Neid peeti kõrvalekalleteks nende tohutu juurdepääsu tõttu kapitalile, kõrgelt arenenud riskikapitalitööstusele ja erineva suurusega turule, kuhu nad sisenevad.

Teksti ja dokumendianalüüsi käigus koostasime mõttekaardi, mis aitab paremini mõista erinevate ökosüsteemide vastastikust mõju ning omada struktureeritud ülevaadet osalejate kohast ja rollist. Mõttekaart illustreerib ökosüsteemi loomise keerukust ja väljakutseid kaitse- ja kahese kasutusega (KK) sektorites, eelkõige kui lisaks keskendume kübertehnoloogiatele.



Meie uurimus keskendus Singapuri ja Ühendkuningriigi ökosüsteemidele. Leidsime mitmesuguseid avalikke erainfrastruktuure, millest mõned on välja töötanud eliituurimisorganisatsioonid, mida muidu rahastavad ja toetavad infokiivad luureagentuurid. Samuti nägime nihet keskendumiselt VKEdelt ettevõtjatele. Lisaks intervjueerisime asutajaid, kes on nendes ökosüsteemides oma idufirmad alustanud, neid laiendanud ja sealt lahkunud. Küsisime neilt nende teekondade kohta ja ka mis neile nendes ökosüsteemides meeldis ja mis ei meeldinud. Koos ökosüsteemiga andsid nad ülevaate ka valitsuse ja avaliku sektori algatustest küberjulgeoleku, kaitse ja kahese kasutusega ökosüsteemide valdkonnas. Meie järelduste kokkuvõte nende intervjuude põhjal on:

- peaaegu kõik asutajad läbisid kiirendiprogrammi; mõni läbis kaks;
- ükski neist ei leidnud kasu valitsuse otserahastamisest; nad eelistasid toetusi varajases staadiumis, maksusoodustusi või abi töötajate leidmisel;
- suurim vajadus oli juurdepääs võrgule, turule ja usaldusele kureeritud meetodi kaudu, mille abil idufirmad saaksid klientidega suhelda, vähendades müügitsükleid;
- tehnilised teadmised ja parimad tavad ei olnud kättesaadavad; idufirmad tundsid, et mõned meeskonnad vajavad seda, kuid arvasid, et parimad ettevõtted otsivad ise parimaid tehnilisi mentoreid;
- idufirmad soovisid rohkem rahastamisvahendeid, kuid selliseid, mis teeksid koostööd olemasolevate riski- ja võlainstrumentidega ning ei nõua rakenduste, aruandluse või kasutamisega seoses täiendavaid üldkulusid;
- asutajad alustasid oma ettevõtmisi sõltumata juba paigas olevatest varajase staadiumi ideearenduselementidest; nad alustasid oma ettevõtteid võimaluse alternatiivkulu ja võimalusmomendi alusel.

Seoses valitsuse ja avalike algatustega nendes ökosüsteemides nägime, et viimase 5–7 aasta jooksul on tärganud märkimisväärne arv algatusi ja arvame, et see on üsna korrelatsioonis positiivse mõjuga nende vertikaalis. Samuti oli ilmne, et valitsused soovivad toetada ainult kohalikke kahese kasutusega algatusi, kuna riigi julgeoleku aspekt on endiselt olemas. Ilmselgelt on see mittekohalike idufirmade jaoks tohutu takistus ja seda tuleks Eestis vältida. Kuigi riiklik julgeolek on võtmeelement, mida arvesse võtta, seisneb edu selles õhukeses vertikaalis, et tagada pakkumisnõudluse ohutu ja kiirendatud rahuldamine.

Selle saavutamiseks on raportis välja pakutud 6 erinevat strateegiat.

- Tegevusstrateegia
- Sektori arengustrateegia
- Turulepääsu strateegia
- Fondistrateegia
- Rahvusvaheline strateegia
- Tehnoloogia strateegia

Pärast kahe ökosüsteemi põhjalikku analüüsimist võtavad need strateegiad olemasolevast parima või siis kombineerivad soovitu nimel eri variante. Lõppkokkuvõttes ei garanteeri miski edu ja peame vajaduste katmiseks katsetama, arendama ja hoolikalt rakendama ülaltoodud strateegiaid.

Seoses ökosüsteemi jätkusuutlikkusega teeme ettepaneku suunata enamik avaliku sektori toetavaid jõupingutusi idufirmade arengu varajastele etappidele ning tugineda turu dünaamikale, võttes kasutusele laissez-faire'i lähenemisviisi hilisemates etappides. See näib olevat kooskõlas intervjuudes väljendatud ootustega ja suunaks ökosüsteemi ka erainvesteeringute kasutamise poole, kui see on põhjendatud.

Ökosüsteemi (kaas)rahastamisel on praegu mitmed teadmata tegurid, mis tulenevad EL-is käimasolevatest protsessidest seoses ESIFi ja EDF rahastamisega. Need kaks näivad aga olevat avaliku sektori panuse peamised allikad. Eeldame, et Eesti suudab kaasa lüüa ERDF, InvestEU ja Euroopa kaitseinvesteeringute programmides ning luua sünergiat HEDI-ga (ELi kaitseinnovatsiooni keskus) ökosüsteemi tegevuste ressurseerimiseks.

Lisaks näitavad hiljutised arengud NATO-s lubadusi pakkuda tulevikus kasulikke ressursse, eelkõige seda, et Eesti on DIANA kaasvõõrustaja ning teatati plaanist pakkuda programmis riskikapitali.

Riigiabi juriidiliste aspektide osas leidsime, et enamiku ökosüsteemi toetavaid tegevusi (ja abikõlblikkuse nõudeid) saab koostada riigiabi regulatsioonidega kooskõlas olevaks. Selle põhjuseks on asjaolu, et üldise grupierandi määrusega on sätestatud sobivad erandid VKEdele antava abi, VKEde rahastamisele juurdepääsu võimaldamise, teadus- ja arendustegevuse ning innovatsiooniabi ning koolitusabi valdkonnas.

Lõpuks juhtisime tähelepanu sellele, et intellektuaalomandi õiguste (IPR) haldamine ökosüsteemi tasandil ja ka üksikisiku/idufirma tasandil nõuab kohandatud lähenemist ja strateegiat. Intellektuaalomandi õigused on asutajate/idufirmade põhivara, seetõttu rõhutasime vajadust süsteemi järele, mis võimaldab intellektuaalomandi õigusi optimaalselt ära kasutada. Teeme ettepaneku võimalusel loovutada ajateenijale/asutajale/idufirmale tema poolt teenistusaja jooksul loodud intellektuaalomandi õigused tingimusel, et see on vajalik ja arendatakse edasi ökosüsteemis, välja arvatud julgeoleku kaalutlustel. Lisaks teeme ettepaneku luua küberajateenijate loodud intellektuaalomandi varade hoidla, mida saab pakkuda teistele ökosüsteemis kasutamiseks tasuta/avatud lähtekoodiga litsentsirežiimide alusel, kui nende looja/autor seda ülalkirjeldatud viisil ei taotle. Ülaltoodud ettepanekut saab rakendada asjakohaste litsentsilepingute ja -kokkulepete süsteemi väljatöötamisega.

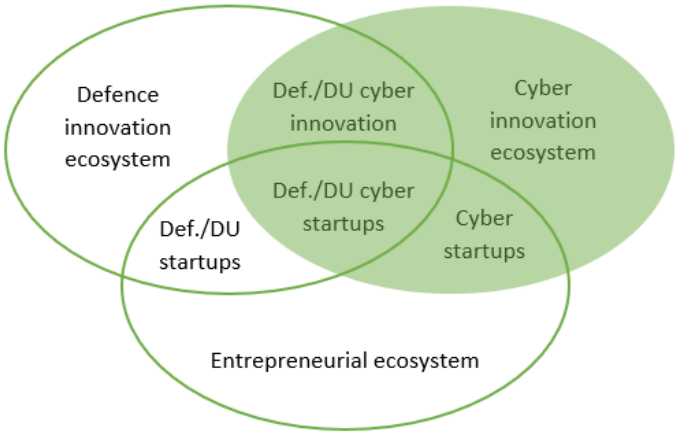
Kokkuvõtlikult võib öelda, et Eesti ökosüsteemis on juba palju võtmeelemente ja praktikaid paigas – ja teostab 2011. aastast tehniliste idufirmade fondiinvesteeringuid AS SmartCapi kaudu; sellel on teatav süvatehnoloogiline infrastruktuur – nt. mitmesugused kübersektorid; on olemas integratsioon ja sünergia teaduse/akadeemiliste ringkondade ja tööstuse vahel töötajate kattumise tõttu ning kaitseklastrid on juba organiseeritud /ja arenevad pidevalt jne. Küll aga soovitab raport nende joondamist ja hästi õlitatud masina viisil koos tööle panemist.

Singapuri ja Ühendkuningriigi küberökosüsteemide uurimisel üht õiget lahendust ei leitud, kuid Eesti on juba käinud sarnasel teel ja omab sarnast praktikat, mis vajab esialgu vaid mõningast kohandamist.

Executive Summary

This is phase two of the project initiated by Call 241018. Phase 1 of the report can be found differently and focused on the success stories of the dual use defence and security startup world. Startups from all over the world in this vertical were analysed to determine which ecosystems Estonia could emulate, what features could be developed and which features should be avoided. Based on the study there, two ecosystems were identified in the **UK and Singapore**. They were the closest to the needs of Estonia and ecosystems like the US and Israel were set aside due to their cash rich position. They were deemed outliers due to their immense access to capital, highly developed venture industry and the different magnitude market that they launch into.

During the desktop research we created a **mind-map** that helps to better understand the interaction between the various ecosystems and have a structured view on the place and role of participants. The mind-map is illustrative of the **complexity** and challenges in creation of ecosystems in the defence and dual-use sectors, in particular with the added focus on cyber technologies.



Our research focused on the Singapore and UK ecosystems. We found the various **public private infrastructure**, some developed by the elite research organisations, otherwise funded and propped up by the secretive intelligence agencies. We also saw the shift from **SMB/SME's to focus on entrepreneurs.** In addition, we interviewed founders who have started, scaled,

and exited their startups from these ecosystems. We asked them about their journeys and what they liked and disliked about their ecosystems. Along with the ecosystem, they also gave insights on the government and public sector initiatives for the cybersecurity, defence and dual use ecosystem. A summary of our **findings from these interviews** is

- Nearly everyone of the founders went through an accelerator program. Some went through two.
- None of them found any use of government funding directly from the government. They preferred early stage grants, or tax relief or employment assistance.
- The biggest need was access to network, market and trust via a curated method by which startups could interact with the customers, reducing sales cycles.
- Technical know how and best practice was unavailable. The startups felt some teams needed this, but felt that the best companies go seek the best technical mentors themselves.
- Startups wanted more funding instruments in place, but ones that collaborated with existing venture and debt instruments, and did not require additional overheads with respect to applications, reporting or usage.
- Founders started their ventures irrespective of the early stage idea development elements in place. They started based on the opportunity cost and time element of the opportunity.

With respect to the government and public initiatives in these ecosystems, we saw a significant number of initiatives being initiated in the **last 5-7 years**, and feel this is quite correlated to the positive impact in the vertical. It was also evident that the governments are keen to support only **local dual use** initiatives as there is still a **national security angle present**. This obviously is a huge hurdle for non local startups and is something to be avoided in Estonia. While national security is a key element to look at, success in this slim vertical is all about making sure supply demand is met in a safe accelerated way.

To achieve this, **6 different strategies** have been proposed in the report.

- Operational Strategy
- Sector Development strategy
- Market Access strategy
- Fund Strategy
- International Strategy
- Technology Strategy

After analysing in depth the two ecosystems, these strategies take the **best of what is there**, what is desired and hope to put it all together. In the end, nothing guarantees success, and we would need to experiment, evolve and execute diligently, the above strategies try to cover the needs.

As to the **sustainability** of the ecosystem, we propose to focus most public sector nurturing efforts on the early stages of startup development and rely on market dynamics, adopting an approach towards laissez-faire in the later stages. This appears to be in line with the

expectations expressed in interviews and would also steer the ecosystem towards the use of private investments where justified.

In **(co-)financing** the ecosystem there are currently several unknown factors due to the ongoing processes in the EU regarding ESIF and EDF fundings. However, these two seem to be key sources for public sector contributions. We expect that **Estonia will be able to tap** into the ERDF, InvestEU, and European Defence Investment Programmes, as well as create synergies with HEDI (Hub for EU Defence Innovation) to resource the ecosystem activities.

Furthermore recent developments in NATO show promises as to offering future useful resources, in particular that Estonia will co-host DIANA and plans were announced to provide venture capital in the programme.

In terms of legal aspects concerning state aid we found that most ecosystem support activities (and aid eligibility requirements) **can be constructed to be compatible with state aid** regulations. This is due to that suitable exceptions are provided by the General Block Exemption Regulation[1] in the field of aid to SMEs, aid for access to finance for SMEs, aid for research and development and innovation, and training aid.

Finally, we pointed out that management of intellectual property rights (IPR) at the level of the ecosystem and also at the individual/startup level requires a tailored approach and strategy. **IPR are key assets** of founders/startups, therefore we emphasised the need for a system that allows the optimal exploitation of IPR. We propose that IPR created by cyber conscripts during their service time to be **assigned to the conscript/founder/startup** under the condition that it is needed and to be further developed within the ecosystem, and unless national security considerations contraindicate the assignment. Furthermore, we propose the creation of a **repository of IP assets** such created by cyber conscripts, which if not pursued by their creator/author as described above, can be offered to others under free/open source licence regimes for exploitation within the ecosystem. The above proposal can be implemented by designing a system of relevant licence contracts and arrangements.

In summary, the **Estonian ecosystem already has many key elements and practices in place** - it does the fund-of-funds investment in tech startups since 2011 via AS SmartCap; it has certain deep-tech infrastructure - eg. various cyber ranges; there is integration and synergies between research/academia and industry due to personnel overlaps, the defence cluster is already organised and developing steadily, etc. However, getting the various **elements to align** and work as a well oiled machine are what are suggested in the report.

There was no 'silver bullet' found during the study of Singapore and UK cyber ecosystems, but Estonia has already been on a similar path and has similar practices, which only need some adaptation initially.

[1] Commission Regulation (EU) No 651/2014 of 17 June 2014 declaring certain categories of aid compatible with the internal market in application of Articles 107 and 108 of the Treaty

1. Introduction

This Phase II report builds on the conclusions of the Phase I report, where Singapore and the UK were identified in order to study and analyse their defence and dual use ecosystems, including cyber ecosystems.

The structure of this report is as follows. Chapter 2 outlines some key terms and concepts relevant to startup ecosystems in order to devise a consistent vocabulary and understanding for the content of this report. Chapter 3 and 4 respond to the research question nr 4.1 in the technical description document (Annex 1 to the Procurement Contract), and elaborates on the models from Singapore and UK, presenting successful examples of the defense and dual-use sectors, including start-ups, for the creation of an ecosystem (including on the basis of cyber-service). Chapter 5 presents the results of interviews conducted with experts, founders, stakeholders in the field. Chapter 6 provides responses to research questions 4.2-4.6. It outlines proposed principles and strategies for the creation of an Estonian defence and dual-use startup ecosystem based on the analysis of the two country models, interviews, experience of the authors in the startup ecosystems and considering further texts and documents used in the study. The division of roles of different parties in the ecosystem is suggested in an integrated manner. The proposals in chapter 6 are departing from the need for self-sufficiency, which is an underlying feature of the entire study. Self-sufficiency is also explicitly addressed in conjunction by two parts - section 6.2.4 Fund Strategy and 6.3. Options and models for co-financing the ecosystem. Finally, section 6.4. addresses legal aspects, focusing on the highlighted areas in research question nr 4.6.

The research process followed the main suggestions in the technical description. Considerable part of the study is based on publicly available text and document analysis, desk research. Sources included policy documents, databases of legislation, recordings of public statements and minutes of parliamentary discussions, information and calls published on official websites of public agencies, international organisations, as well as major news sites.

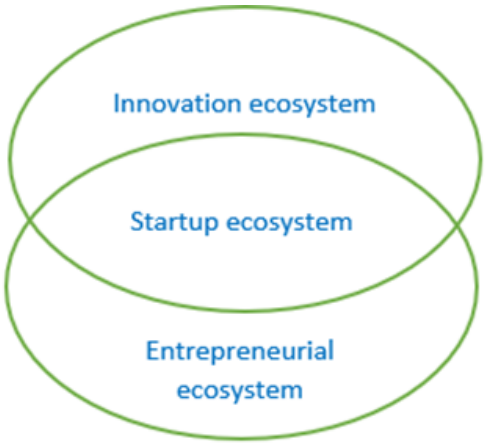
Six Interviews with experts, engaged parties in startup business, founders and others were conducted, however all respondents wished to remain anonymous. It is noted that overwhelming majority of approached potential interviewees showed great reluctance to respond, 4 reconsidered when we explained that the information collected is meant to be used for a government report.

In the study we provide various simulations and consider possible scenarios for aspects of the planned ecosystem. SWOT analysis is also provided for the operational strategy. Additionally, the relevant legal environment and related risks are considered with main focus focus on IPR and state aid, as well as mentioning some other potential legal issues.

2. Setting the scene

For several years now the innovation process has been moving away from „closed structures“ from big companies and organisations (eg. universities) to more **open and collaborative** ecosystems. In the networked world, innovation via startups is fast, flexible, highly motivated, cost effective and supported by private and public sector partners. There is an expectation of constant innovation in the digital economy and new and young companies generate almost all private sector jobs.[2][1]

The term ’ecosystem’ tries to communicate an analogy from nature, so one that is not to be controlled by anyone, not owned, yet it always exists when there is activity. Ecosystem is a type of invisible infrastructure around the actors and activities that are taking place. **Startup ecosystem is a combining factor between innovation ecosystem and entrepreneurship ecosystem**, combining the ingredients, actors and activities from both worlds.



Countries are competing to have world’s leading startup ecosystems to sustain their economy and a startup ecosystem can be seen as the „R&D department“ of a country, which serves home markets and beyond. It can be achieved when all startup ecosystem organisations and roles are well-networked, and there is transparency of different actors in the field.

‘Startup’ is a **dynamic category**, not lending itself to the traditional labelling of companies (such as micro, SME, large, etc), and can be best understood as a process of innovation and growth by design. Key factors for startup development are multiple, including market opportunity, market timing, team commitment, team structure, scalability, growth ambition, and a startup ecosystem needs to take a balanced development perspective to support these. The main failure factor for startups is premature scaling, meaning going too far in any one dimension, while the other aspects are left underdeveloped (eg. too big team too early, too many customers too early without corresponding support functions).

[2] Kaufmann Foundation

Startup development can be broadly divided into three phases, and when looking to develop a startup ecosystem, activities in all these phases need to be targeted in a structured and balanced way and with a long-term view.

Source: Startup Commons

Startups innovate to do real business, but they also develop a new growing organisation, hence both innovation/business and team are key aspects, which need to be in sync.

3. Singapore

3.1. Snapshot

Singapore has a population of 5.5 million people, the city-state is ranked at the top of the list of the world's most competitive economies and became an innovation hotspot attracting entrepreneurs and startups. The government has a strong **interventionist** policy aimed at driving economic growth and enabling sectors and firms that it considers crucial to the country's long-term economic prospects.[3]

Singapore has been experiencing an **exponential growth in technology startups** and digital transformation in its core industries. Singapore has been consistently delivering peak innovation performance, it is the 2nd most innovative country in the region and ranks at the 8th position globally (Estonia is 21st).[4] Singapore ranked 1st in the world in terms of the 'Institutions' pillar of the Global Innovation Index, and 18th among the global startup ecosystems[5] with 11 new unicorns in 2021, which makes it a useful case-study for the purposes of this report.

In the 2020 Singapore Public Sector Outcomes Review, which takes stock of how Singapore has fared in key areas of national interest from a citizen's and business' perspective,[6] the main achievements in the security domain were focusing exclusively on digital and

[3] Economist Intelligence, Singapore fact sheet http://country.eiu.com/article.aspx?articleid=642047847&Country=Singapore&topic=Summary&subtopic=Fact+sheet

[4] WIPO Global Innovation Index 2021 (UK overall GII rank is 4th, institutions pillar 15th)

[5] Startup Genome report 2021 https://startupgenome.com/ecosystems/singapore

[6] https://www.mof.gov.sg/singapore-public-sector-outcomes-review/businesses/ease-of-doing-business/security

cybersecurity. This illustrates the holistic importance of cybersecurity in Singapore with the following highlights:

- Cybersecurity readiness in Deloitte's Cyber Smart Index Singapore was the first, and secure and safe cyberspace is seen as the foundation for a strong and stable digital economy;
- Cybersecurity Authority working closely with the 11 critical information infrastructure sectors and establishment of Operational Technology Information Sharing and Analysis Centre;
- Helping businesses secure their digital spaces via various platforms and funding support;
- Boosting the cybersecurity ecosystem by increasing the skilled cyber workforce, establishing the region's first cybersecurity entrepreneur hub and launching the Cybersecurity Innovation and Growth Programme.

EGA National Cybersecurity Index[7]		ITU Global Cybersecurity Index	
2019	7	2017	1
2020	12	2018	6
2022	15	2020	4

Table 1. Singapore's ranks on cybersecurity indexes

With more focus on the defence domain, the national cyberpower index 2020 worked out by Belfer Institute at Harvard University puts Singapore at 18th place (Estonia 14th), however according to the Cyber Capability Index the city-state ranks 7th (and under the defense objective the 2nd most capable after China). Table 2. below indicates the various cyber capability objectives and top 10 countries.

However, the Singaporean defence objective needs a bit of clarification, in particular that the country does not feature in the offence column. Several scholars emphasised that the military is dominated by the civilian sector as an integral part of the state's administrative structure, forming a symbiotic relationship by today.[8] Driven by the complexity of security challenges (and the wicked problems and black swans generated by complexity) the Singaporean government adopted the **whole-of-the-government approach**, which implicitly contains the idea that it is not possible for everything to be centrally directed.[9] The presence of ex-military officers in the cabinet, civil service and statutory boards is believed to be the reason for the center of gravity for the Singaporean approach to cyberspace. The

[7] https://ncsi.ega.ee/country/sg/549/#details

[8] Ross Worthington, Governance in Singapore (London: RoutledgeCurzon, 2003). Stephen McCarthy, The Political Theory of Tyranny in Singapore and Burma: Aristotle and the Rhetoric of Benevolent Despotism (New York: Routledge, 2006).

[9] Peter Ho, Governing for the Future: What Governments can do, S. Rajaratnam School of International Studies Singapore, Working Paper Nr. 248. 3 September 2012.

government is also able to control and co-opt the private sector into national security matters through public-private partnerships.[10]

Cybersecurity Agency is geared toward combating cyber-attacks on critical infrastructure sectors, but online cyber-criticism of government policies and online radicalization is also perceived as a potential challenge to legitimacy of the ruling party and societal stability. Both these challenges, while different in nature, are seen by the government to stem from the cyberspace ecosystem that needs to be better regulated.[11] However, the government's restrictive attitude towards criticism also appears to be an obstacle in objectively assessing the current ecosystems, since the approached stakeholders and their representatives have been reluctant to share their experiences on topics related to this study.

#	Surveillance	Defense	Information Control	Intelligence	Commercial	Offense	Norms
1	US	China	US	US	US	Russia	US
2	UK	Singapore	Russia	UK	South Korea	US	France
3	France	Canada	China	China	China	China	Japan
4	China	France	South Korea	Germany	Japan	Germany	China
5	Japan	Switzerland	Sweden	Singapore	UK	UK	Germany
6	Sweden	Netherlands	Singapore	Israel	Singapore	France	Singapore
7	Canada	US	UK	France	Netherlands	Netherlands	UK
8	Germany	Japan	New Zealand	Malaysia	Germany	Spain	Malaysia
9	New Zealand	Germany	Saudi Arabia	Estonia	France	Estonia	South Korea
10	Israel	Sweden	Canada	Netherlands	Switzerland	Canada	India

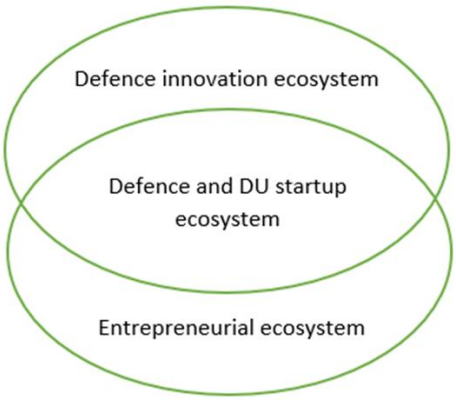
Table 2. Cyber Capability Index 2020. Source: National Cyber Power Index 2020, Harvard Kennedy School Belfer Center for Science and International Affairs[12]

[10] Syed Mohammed Ad'ha Aljunied (2020) The securitization of cyberspace governance in Singapore, Asian Security, 16:3, 343-362, DOI: 10.1080/14799855.2019.1687444

[11] Syed Mohammed Ad'ha Aljunied (2020) The securitization of cyberspace governance in Singapore, Asian Security, 16:3, 343-362, DOI: 10.1080/14799855.2019.1687444

[12] https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

3.2. Key stakeholders in the defence and dual-use (DU) startup ecosystem and their roles:



Government sector:

Research, Innovation and Enterprise ecosystem (RIE) in Singapore comprises various ministries, R&D funding bodies and R&D performers. At the top is the Research, Innovation and Enterprise Council (RIEC), chaired by the Prime Minister, which oversees the long term strategy to transform Singapore into a knowledge-based society, with strong capabilities in research and technology. The RIEC is supported by the National Research Foundation (NRF) Board, which is responsible for the formulation of the 5-year plans and policies to grow Singapore's research capability, support economic growth and meet Singapore's future national challenges.

National Research Foundation (NRF) was created in 2006 and is a department within the Prime Minister's Office. Its task is to set the R&D direction for Singapore through the development of policies and strategy for research and innovation. It funds strategic initiatives and its efforts are organised around four strategic domains, supported by three cross-cutting horizontals:

- Manufacturing, Trade and Connectivity
- Human Health and Potential
- Urban Solutions and Sustainability
- Smart Nation and Digital Economy

Horizontals: Academic research, Manpower, Innovation and Enterprise

According to Singapore's newest R&D strategy, RIE2025, the government will sustain investment in research, innovation and enterprise at about 1% of the GDP ($25B) over 2021-2025.

NRF offers fellowships at local universities and research institutions, NRF investigatorships, competitive research programmes, but it also has innovation and enterprise-oriented schemes. For example, its Early Stage Venture Fund (ESVF) seeds funds with selected venture capital firms to invest in Singapore-based early-stage technology start-ups. Under this initiative, the NRF invests S$10 million on a matching basis, to seed corporate venture

capital (VC) funds that invest in Singapore-based early stage high-tech companies. As an incentive, the corporate VCs have the option to buy out NRF's share of the fund within five years by returning NRF's capital with interest.[13] NFR also runs the Central Gap Fund ("Central Gap") initiative. It aims to support the translation of research outcomes into products, processes and/or services that generate economic and societal benefits for Singapore. Central Gap provides funding up to S$2M for 2 years, and it only supports projects that have high impact and significant value for Singapore, and that are nearing commercialization/use. The project teams must have experienced business/development persons on board (or available as mentor). NRF also runs the National Cybersecurity R&D programme (see details in section 3.3).

The RIE2025 plan Innovation and Enterprise horizontal if focusing on growing a vibrant national innovation ecosystem, driving translation and boosting capabilities. Some of the measures include the Open Innovation Network (OIN),[14] which is a portal bringing together innovation challenges and community partners. Corporates and government agencies can share their pain points or business needs on the OIN; innovators can respond to, co-develop and test-bed new solutions with the problem statement owners.

Further aims in the RIE2025 plan are the scale-up and strengthening translation platforms[15]; and forging strong connections to major innovation hubs and key demand markets. The latter aim appears to be indispensable, given Singapore's resource constraints and small domestic markets. Therefore strong international networks and exposure for Singapore enterprises are key to maintaining and providing access to global and regional markets, innovation expertise and resources, and Singapore has been building the Global Innovation Alliance since 2017. NRF's schemes and initiatives aimed at SME, startup funding and grants are generally offered via Enterprise Singapore.

Enterprise Singapore[16] is the government agency for enterprise development and it is part of the Ministry of Trade and Industry. It works with companies to build capabilities, innovate and internationalise. It offers various financial and non-financial assistance in a very broad range of industries, including digital/ICT, and cybersecurity.

Various StartupSG funding opportunities are offered, including StartupSG Founder Grant[17] (up to $50,000 cash against nominal percentage in equity if additional $10,000 can be secured), or StartupSG Tech Grant[18] is early-stage funding up to $500,000 for commercialization of deep tech proprietary technology, and it carries an equity component where Enterprise Singapore will have the rights to exercise a share subscription. Besides the grants, Enterprise Singapore has programmes to enable access to loans and insurance (by private partners), administers some tax incentives (approval needed), and provides

[13] https://www.nrf.gov.sg/funding-grants/early-stage-venture-fund
[14] https://www.openinnovationnetwork.gov.sg/
[15] Such as Diagnostics Development Hub and the National Additive Manufacturing Innovation Cluster.
[16] https://www.enterprisesg.gov.sg/
[17] https://www.startupsg.gov.sg/programmes/4894/startup-sg-founder
[18] https://www.startupsg.gov.sg/programmes/4897/startup-sg-tech

investments. It runs the StartupSG Equity Grant[19], which provides co-investment opportunities for startups and investors. The government can co-invest with independent, qualified third-party investors into eligible startups; or invest in selected venture capital firms that in turn invest in eligible startups. Enterprise Singapore offers the Gov-PACT programme, which is an opportunity for SMEs/Startups to supply solutions to the government upon their call.[20] Such calls have also originated from the Defence Science & Technology Agency, DSTA.[21]

Investment Parameters		
	General tech	Deep tech
Investment Cap for each startup	$2M from SEEDS Capital	$8M from SEEDS Capital
Co-investment ratio	7:3 up to the first $250K from SEEDS Capital; 1:1 thereafter, up to $2M	7:3 up to the first $500K from SEEDS Capital; 1:1 from $500K to $4M 3:7 thereafter, up to $8M

Table 3. Investment parameters under the StartupSG Equity Grant. Source: https://www.startupsg.gov.sg/programmes/4895/startup-sg-equity

Economic Development Board is a government agency under the Ministry of Trade and Industry and it is responsible for developing and implementing strategies designed to enhance Singapore's position as a global centre for business, innovation, and talent. It is better known for its later-stage investments, EDBI is the dedicated corporate investment arm of the EDB, and a global investor in select high growth technology sectors covering Information & Communication Technology (ICT), Emerging Technology (ET), Healthcare (HC) and other strategic industries. For example it offers the Special Situation Fund for Startups via convertible note, which may have developed technologies and innovations that can contribute to Singapore's national priorities.[22]

Success story of Transcelestial

Singapore-based deep tech startup has raised US$9.6 million in a Series A funding round co-led by EDBI, and existing investor Wavemaker Partners.

The round drew new investors Airbus Ventures, Cap Vista, which is the strategic

[19] https://www.startupsg.gov.sg/programmes/4895/startup-sg-equity
[20] https://www.ipi-singapore.org/esg/challenge/1043/enterprise-singapore-innovation-call-to-seek-solutions-for-intelligent-web-crawler-2
[21] https://www.ipi-singapore.org/esg/challenge/28/statement-details-20.html
[22] https://www.edb.gov.sg/en/how-we-help/incentives-and-schemes.html

investment arm of the Defence Science and Technology Agency of Singapore, and global venture capital (VC) firms Partech and Tekton Ventures.

Existing investors talent incubator Entrepreneur First, Enterprise Singapore's SEEDS Capital, as well as angel investors Charles Songhurst, Microsoft's former head of corporate strategy, and Ajay Shah, a program manager at Standard Chartered, also participated in the round.

Transcelestial is working on delivering high-speed Internet through a laser network in space. Its goal is to eventually deliver Internet connectivity at up to 100 gigabits per second (Gbps), hundreds of times faster than conventional speeds seen today.

Sources:
https://www.capvista.com.sg/news/wireless-laser-communications-startup-transcelestial-snags-us9-6m-from-edbi-wavemaker/

https://www.transcelestial.com/

Ministry of Defence (MINDEF) brings together the **Defence Technology Community**, which forms integral part of the Defence Technology Ecosystem.

Source: Ministry of Defence

The Singaporean Defence Technology Community comprises of several entities within MINDEF: Future Systems & Technology Directorate (FSTD), Technology Strategy & Policy Office (TSPO), Industry & Resources Policy Office (IRPO) and Defence Technology Collaboration Office (DTCO) – as well as Defence Science and Technology Agency (DSTA) and DSO National Laboratories. Two entities are highlighted below from this structure, the DSO National Laboratories and the DSTA.

DSO National Laboratories is Singapore's largest defence R&D organisation with the critical mission to develop technological solutions to sharpen the cutting edge of Singapore's national security. It invests $250 million yearly into R&D and employs over 1000 research scientists and engineers working across the domains of land, sea, air, space and cyberspace.

Information Division focus on cyberspace technologies.[23] DSO works closely with Singapore's universities and local facilities and local partners, including ST Engineering (over 50% owned by Singapore Government via Temasek Holding).

Defence Science and Technology Agency (DSTA), is a statutory board and procurement agency under Singapore's Ministry of Defence. It somewhat corresponds to the Centre for Defence Investment (Riigi Kaitseinvesteeringute Keskus) in Estonia. The DSTA performs acquisitions management, systems management, systems development for the Singapore Ministry of Defence and the Singapore Armed Forces. It has 18 programme centres from Air Systems through Cybersecurity to Information and Infocomm Infrastructures and offers various opportunities to students, researchers (internships, scholarships, competitions), as well as to industry partners (procurement). DSTA's strategic investment arm is Cape Vista Pte Ltd that is focused on defence domain (another government owned VC is SGInnovate focusing on deep tech[24]).

Cap Vista Pte Ltd[25]

In 2020 the government announced a S$300 million support for the deep-tech startup ecosystem. One way that the Defence Technology Community helps to grow companies in the defence and security ecosystem is through Cap Vista Pte Ltd. Cap Vista is the strategic investment arm and fully owned subsidiary of the DSTA, a corporate VC fund founding early-stage deep tech startups. It provides equity-related or project-linked financing to start-ups with innovative technologies that can serve the defence and security needs of Singapore. Beyond investment capital, Cap Vista provides strategic and technical advice to help start-ups maximise their opportunity for success. Although it is a VC, making money like a typical fund is not a primary goal, but to get the technology to put to use in the ministry, armed forces, or the government agencies that we work with. "Everyone is waiting for someone to initiate investing in a new company," CEO Zhen Hao Chng pointed out. "So we want to be the one who is leading this investment into deep tech."

Portfolio of Cap Vista[26]:

BeeX	https://beex.sg
Bifrost	http://bifrost.ai/
Transcelestial	https://transcelestial.com/
Aliena	http://www.aliena.sg

[23] https://www.dso.org.sg/research/information
[24] https://www.sginnovate.com/
[25] https://www.capvista.com.sg/
[26] https://www.capvista.com.sg/our-portfolio/

Insider Security	http://insidersecurity.co
TandemLaunch	http://www.tandemlaunch.com
Atomionics	http://www.atomionics.com
Subnero	http://subnero.com
Microfine Materials Technologies	http://www.microfine-piezo.com
Seventh Sense	http://www.seventhsense.ai

Under the **Ministry of Home Affairs** a new Science and Technology Agency was established in 2019 - **Home Team X** (HTX).[27] The budget for Home Team agencies is set to double by 2025 (up to $1.9B) and it was reasoned by the Minister of Home Affairs that a new agency will allow capability development in-house.[28] Home Teams have been the recipients of some DSO-developed technologies, and the HTX allows to stay ahead in areas such as forensics, biometrics and surveillance, and also to calculate with the unique requirements in this field. Existing agencies like the DSO, DST, even though they are dedicated and separate, they do not operate in silos and they do cooperate very closely with one another - according to Minister Teo.[29] The HTX has a cybersecurity centre of expertise, which is part of the cybersecurity ecosystem.[30]

Finally, MINDEF is active in engaging the entire society, and runs various total defence campaigns. One recent initiative is the **Total Defence Sandbox**[31] introduced in February 2022, a new platform that enables the public to share ideas on strengthening total defence and have their ideas brought to life through funding or match-making.[32]

Government Technology Agency (GovTech)[33] was launched in 2016 to harness the use of technology in governmental services. Their focus is on 6 key areas, being data science, government infrastructure, application development, geospatial technology, cybersecurity

[27] https://www.htx.gov.sg/

[28] https://www.straitstimes.com/politics/mha-budget-on-boosting-home-team-agencies-capabilities-to-double-to-19-billion-in-2025

[29] https://www.mha.gov.sg/mediaroom/parliamentary/wrap-up-speech-of-the-home-team-science-and-technology-agency-bill---speech-by-mrs-josephine-teo-minister-for-manpower-and-second-minister-for-home-affairs/

[30] https://www.htx.gov.sg/expertise/our-expertise/cybersecurity

[31] https://www.ideas.gov.sg/public/tdsandbox

[32] https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/February/12feb22_nr2

[33] https://www.tech.gov.sg/

and smart sensors. GovTech is also the cybersecurity lead to the governmental sector and its Cyber Security Group delivers a full spectrum of technical and operational capabilities in this field.[34]

Academia:

There are two very high ranking universities in Singapore. **National University of Singapore** (NUS) ranks 11th, **Nanyang Technological University** (NTU) 12th in the world in 2022.[35]

NUS Enterprise is the entrepreneurial arm of NUS and plays a pivotal role in advancing innovation and entrepreneurship in Singapore. NUS Enterprise does not only run educational programs, but also provides support to entrepreneurs at early and growth stage and it boasts an entire comprehensive innovation & enterprise ecosystem.[36] Many of its activities and programmes are funded by NRF and NUS Enterprise partners up with industry. NUS is home to the Temasek Laboratories since 2000 in partnership with the Ministry of Defence, and it complements the DSO National Laboratories and the local defence industry. Temasek Lab has 'sisters' at NTU and SUTD. In 2018 NUS reported to set up a new collaboration space with DSTA to partner local start-ups to develop solutions for Singapore's defence and security, the DSTA@71 lab.[37] In a call issued in 2019 the opportunity was given to selected teams to apply for GOV-Pact grants with Enterprise Singapore.[38]

NUS also hosts the Cybersecurity Laboratory and Singtel Cybersecurity R&D Lab. The National Satellite of Excellence in Trustworthy Software Systems under the National Cybersecurity R&D programme is hosted at NUS and co-led by NTU.

NTU commercialises 30% of its research and 40% of its work leads to a spin-off and their ambition is to collaborate further with industry, with 30% of its research activity being formed with government agencies.

The National Satellite of Excellence, **iTrust - Centre for Research in Cybersecurity**[39] was established in 2012 by the Singapore University of Technology and Design (SUTD) and the Ministry of Defence. iTrust's research focuses on the development of advanced tools and methodologies to ensure the security and safety of current and future systems in five thrusts: Cyber Physical Systems (CPS), Internet of Things (IoT) systems, Enterprise Networks, Autonomous Vehicles, and Blockchain. SUTD also hosts and leads the National Satellite of Excellence in Design Science and Technology for Secure Critical Infrastructure, an NRF-supported programme focusing on advancing the state of the art and state of practice in the design of secure and safe critical infrastructure.[40]

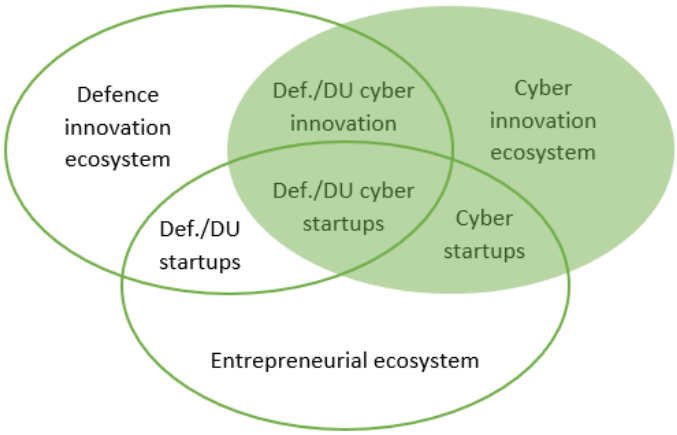
[34] https://www.tech.gov.sg/capability-centre-csg
[35] https://www.topuniversities.com/university-rankings/world-university-rankings/2022
[36] https://enterprise.nus.edu.sg/education-programmes/nustap/
[37] https://www.nus.edu.sg/newshub/news/2018/2018-10/2018-10-31/DEFENCE-st-31oct-pB2.pdf
[38] https://www.dsta.gov.sg/docs/default-source/blk71/inno-call_challenge-statement_190212.pdf
[39] https://itrust.sutd.edu.sg/
[40] https://itrust.sutd.edu.sg/nsoe-destsci/

Industry and collaborative efforts:

Block71 is a technology-focused ecosystem builder and global connector which catalyses and aggregates the start-up community. It is an initiative of NUS and it collaborates with established corporates and government agencies. It offers incubation/acceleration programmes, access to NUS research capabilities and patented technologies and exposure to NUS Enterprise's wide network of venture capitalists, investors, industry partners and mentors. Block71 programmes include startup support in industry collaborations in the fields of defence (DSTA@71) and cybersecurity (ICE71) and others.

SingTel Innov8 (Innov8), a wholly-owned subsidiary of the SingTel Group, is a corporate venture capital fund and co-founder of Block71. It has a fund size of US$250 million, with presence in Singapore, Silicon Valley, Tel Aviv and other markets. Innov8 focuses its investments on technologies and solutions that lead to quantum changes in network capabilities, next-generation devices, digital content services and enablers to enhance customer experience.

3.3. The cybersecurity ecosystem



There is significant overlap between the different ecosystems due to the dual-use nature of information and communication technologies. Defence-related innovation ecosystem has a strong cyber element, however a distinct cybersecurity ecosystem has also been designed, which naturally extends beyond the defence domain.

Since 2013 the city-state's direction for cybersecurity is to develop R&D expertise and capabilities to improve the trustworthiness of cyber infrastructures and systems with an emphasis on security, reliability, resilience, and usability among government agencies, academia, and industry. Since 2015 the Prime Minister's Office Strategy Group[41] has been a focal point for providing overall organisational command and control of technology, security and other strategic policies for Singapore.

[41] https://www.strategygroup.gov.sg/

Cybersecurity Authority of Singapore (CSA) was formed in 2015 and has been given the task of protecting Singapore's cyberspace. It is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information. The CSA oversees cybersecurity strategy, operation, education, outreach, and ecosystem development. Core mission of the CSA is to keep Singapore's cyberspace safe and secure, to underpin National Security, power a Digital Economy, and protect the Digital Way of Life.

CSA works closely with industry and the universities to encourage cybersecurity innovation, and deliver solutions, and it also collaborates with education institutions and industry partners to build a robust cybersecurity workforce, to meet the growing demand to secure the digital economy. The criteria set for the ecosystem is that it needs to be a sustainable source of expenditure and solutions, bring about economic opportunity and jobs. CSA has a commitment to advance capabilities through R&D. This is achieved through the Cybersecurity Co-Innovation and Development Funding Scheme.

In 2021 the CSA has established the Operational Technology Cybersecurity Expert Panel (OTCEP)[42] comprising 11 local and international Operational Technology (OT)[43] cybersecurity experts. This allows Singapore's OT cybersecurity practitioners, operators, Industry, researchers, and policy makers from the Government, Critical Information Infrastructure (CII) sectors, academia and other OT industries to have direct access to internationally renowned experts, draw from their experience, insights and recommendations.

The newest Cybersecurity Strategy of 2021[44] pledges to develop a vibrant **cybersecurity ecosystem**, which includes the 1) development of advanced capabilities for economic growth and national security, 2) innovating to build word-class products and services, as well as 3) growing the cybersecurity market. The vibrant cybersecurity ecosystem is seen as one of the foundational enablers of Singapore's overall objectives[45] - the other foundational enabler is the robust cyber talent pipeline. Therefore, the industry and academia-oriented entrepreneurial approach is strongly interlinked with the development of the **cyber workforce**.

Cybersecurity ecosystem pillars:

1) The development of advanced capabilities is focused on two main points, and a key vehicle for both is the National Cybersecurity R&D Programme (NCR), which is augmented by attracting top international companies.

    a) The translation of research into innovative and economically viable products using programmes such as the Lean Launchpad programme or the Seed Grant at Cybersecurity Consortium;

[42] https://www.csa.gov.sg/Who-We-Are/committees-and-panels/operational-technology-cybersecurity-expert-panel

[43] Operational Technology (OT) refers to technologies involving interconnected devices and computers for the monitoring and control of physical processes.

[44] https://www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021

[45] I.e. 1. Build resilient infrastructure, 2. Enable safer cyberspace, 3. enhance international cooperation.

b) The build up of deep capabilities - eg. the National Cybersecurity R&D Lab, which is a shared national infrastructure that provides computing resources, repeatable and controllable experimentation environments, as well as application services.

2) Innovation to build world-class products and services has three focal points.

   a) The support for industry-led innovation is targeting established cybersecurity firms with programmes such as the Cybersecurity Industry Call for Innovation, where innovation is matched with the local needs (eg. CII owners).

   b) The encouragement and support for innovators and startups is concentrated around the Innovation Cybersecurity Ecosystem at Block 71 (ICE71) initiative.

   c) International recognition of local security products in the global marketplace is fostered by product evaluation, testing and certification facilities and by the establishment of National Integrated Centre for Evaluation (NICE). Singapore is evaluating and certifying products against the international Common Criteria standard and has a Cybersecurity Labeling Scheme for consumer smart devices. The next steps are focused on the accessibility of advanced equipment required for security evaluation and supporting the growth of the local testing, inspection and certification (TIC) industry, as well as building up local expertise in this field.

3) Growing the cybersecurity market entails the building of demand for cybersecurity solutions, for example by subsidizing the adoption of pre-approved cybersecurity solutions under the SMEs Go Digital Programme or by match-making between suppliers and larger organizations with specific needs. Singapore is looking to support expansion of promising cybersecurity companies overseas and exporting Made-in-Singapore solutions.

The **National Cybersecurity R&D Programme** (NCR) is coordinated by National Research Foundation Singapore (NRF), National Security Coordination Secretariat, Cyber Security Agency of Singapore, Ministry of Home Affairs, Ministry of Defence, Government Technology Agency, Info-communications Media Development Authority (IMDA) and Economic Development Board to promote collaboration among government agencies, academia, research institutes and private sector organisations. The funding of NCR was near to $ 200 million over eight years and it includes grant calls and cybersecurity research infrastructure.

NCR supports a synergistic range of initiatives to advance the technological state-of-the-art in the National Satellites of Excellence in universities, grants for local research projects, international research collaborations, and joint technology developments with industry. Innovation is fostered through cross-sector R&D discussions and partnerships and fast-

tracked by national testbeds for safe and repeatable cybersecurity experiments.[46] The ecosystem support plays an important role in ensuring that research is impactful and responsive to cybersecurity needs of the industry and the society, thus characteristically co-creation is strongly favored.

National Cybersecurity R&D Programme Grant Calls run yearly since 2017. Three key priorities in cybersecurity R&D have been identified for the grant call, namely, National Security, Critical Infrastructure and Smart Nation. The emphasis of the grant call is on the translational and deployability of ideas and technologies. Dual use of new capabilities outside of the Public Sector is encouraged. To ensure scientific rigour and commercialisation capacity, only proposals submitted by Singapore-based companies in collaboration with Institutes of Higher Learning, research institutions or government agencies are eligible.[47]

The CSA is currently running the third cycle[48] of Cybersecurity Call for Innovation[49], financed under the Cybersecurity Co-Innovation and Development Funding Scheme. Up to $1 million per project can be awarded for 24 months to Singapore registered companies that can secure at least one committed cybersecurity end-user for the codevelopment of a minimum viable product and/or market ready technology. At least 50% of the project should be carried out by Singapore's workforce and Singapore should be the base for registering/holding intellectual property. Funding is on a cost reimbursement basis, eligible costs are expenditure on manpowery, equipment and professional Services. This scheme is open to organisations from overseas; however, they must partner with a legal entity in Singapore.

Singapore set up three **National Satellites of Excellence**, on Trustworthy Software Systems at the National University of Singapore, on Mobile Systems Security at the Singapore Management University, and on Secure Critical Infra-structure at the Singapore University of Technology and Design. These satellites provide strategic thrusts in a focus area and help to develop the research and innovation ecosystem in Singapore, working closely with various national initiatives such as the Singapore Cybersecurity Consortium.

The **Singapore Cybersecurity Consortium** is a national engagement platform for the research community, industry, and public agencies to discuss and collaborate in technology adoption and research translation to solve cybersecurity challenges. It is funded under the NCR and is hosted by the National University of Singapore.[50] Its primary role is to bridge the different sectors in driving the flow of innovations from research to market. Firstly, by helping companies and agencies navigate the various research and technology developments. Secondly, by exposing researchers to industry and market perspectives. Operating environment challenges and research outcomes are discussed in thematic Special Interest

[46] Karen Teh, Vivy Suhendra, Soon Chia Lim, and Abhik Roychoudhury. 2020. Singapore's cybersecurity ecosystem. Commun. ACM 63, 4 (April 2020), 55–57. https://doi.org/10.1145/3378552

[47] https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme

[48] 2nd cycle: https://tnb.vc/event/signature-csi/; 3rd cycle: https://www.csa.gov.sg/Programmes/Co-Innovation-Development-Fund

[49] https://cybercall.sg/

[50] https://sgcsc.sg/

Groups (members only).[51] Through these interactions, researchers and companies identify common unresolved problems, and form partnerships for joint research and codevelopment, some of which can be funded by the Consortium's annual **seed grant** (so far 14 projects were funded). Seed grant is for joint industry-academia research projects for producing proof-of-concept and member companies may jointly submit a proposal with academic/research institutes or public agencies. As its future work, the Consortium hopes to tackle the prevalent last-mile gap in research translation efforts, in particular coordinating manpower and training efforts.[52]

Singapore has set up the **National Cybersecurity R&D Laboratory** (NCL) in 2017, which is a shared facility hosted at the National University of Singapore boasting a wide range of ready-to-use tools for security testing, predictable experimentation environments and useful datasets for conducting and validating research ideas and cybersecurity solutions. iTrust Labs, which was set up to conduct multidisciplinary research in cyber-physical systems at the Singapore University of Technology and Design's, has joined the NCL platform in 2019. Collectively, the NCL and iTrust Labs offer integrated experimentations and services to support government agencies, academia and industry in their enterprise IT and operations technology cybersecurity research, technology evaluations and training. Research teams from academia and industry seeking to commercialise cybersecurity technologies are mentored on customer discovery and product positioning in the **Lean LaunchPad Singapore**: Cybersecurity Track, which integrates both business and technological perspectives. Lean LaunchPad is a 10 week immersive programme to help researchers discover and validate the commercialisation potential of their technologies.

This is complemented by the **Innovation Cybersecurity Ecosystem at Block 71 (ICE71)**, which provides entrepreneurship, accelerator, upscaling programs for startups. ICE71 is the region's first cybersecurity entrepreneur hub founded by NUS-Enterprise (the entrepreneurial arm of the National University of Singapore) and Singtel Innov8 (the venture capital arm of the Singtel Group), and supported by the Cybersecurity Agency and community partners.

It aims to strengthen Singapore's growing cybersecurity ecosystem by attracting and developing competencies and deep technologies to help mitigate the rapidly increasing cybersecurity risks in the region. Supported by the CSA, it is Singapore's first integrated cybersecurity entrepreneur hub, supporting and developing early and growth stage cybersecurity entrepreneurs and startups from around the world.

ICE71 runs various programmes, the three main ones are ICE71 Inspire, ICE71 Accelerate, ICE71 Scale and ICE71 Community. ICE71 Inspire and ICE71 Accelerate are run by CYLon, the leading global accelerator and investor in early-stage startups. ICE71 Scale is designed to help international and local startups to grow their businesses and each start-up will have access to office space and facilities, the opportunity to leverage longer term support and

[51] https://sgcsc.sg/special-interest-groups/

[52] Dr Vivy Suhendra, Executive Director of the Singapore Cybersecurity Consortium, FOSTERING CYBERSECURITY CO-INNOVATION, NRF Magazine november 2021.

expertise by way of mentoring, networking events, workshops, and access to go-to-market channels and cybersecurity resources. ICE71 Community is focused on knowledge sharing and networking via tailored events. NUS-Enterprise also channels various government non-cyber-specific opportunities (e.g. ones offered by Enterprise Singapore) into ICE71.

Important element of the ecosystem is that Singapore positioned itself as a regional cybersecurity hub and attained the status of a **Common Criteria Certificate Authorizing Nation** in 2019. This allows lower costs and shorter time for developers to get certified and facilitates the export of cybersecurity products produced locally.

3.4. Select legal aspects

Singapore has a National IP Protocol that took effect in 2018, and contains the IP Principles for Publicly Funded R&D.[53] These are the followings:

- IP created using public funds shall be managed and utilised with a view to create and capture value, for the benefit of Singapore.
- Public Agencies shall adopt a common framework for industry engagement and how IP shall be owned, protected, used, and commercialised.
- IP created using public funds shall be actively managed to ensure optimal utility.
- Public Agencies should, in general, reserve a royalty-free, irrevocable, worldwide, perpetual and non-exclusive right to use any licensed or assigned IP for their statutory functions, non-commercial and/or R&D purposes. Public Agencies should consider the commercial interest of the third party before applying this principle and act in a manner that supports the effective commercialisation of the IP by the third party.
- Commercialisation of IP created using public funds should also benefit the researchers who are the inventors or creators of the IP.

On a side-note it should be pointed out that Singapore exercises control over certain cybersecurity services based on the Cybersecurity Act[54] and the recent Cybersecurity Service Providers Regulation[55] of April 2022. Licensable Cybersecurity Services are (a) managed security operations centre (SOC) monitoring service; and (b) penetration testing service.

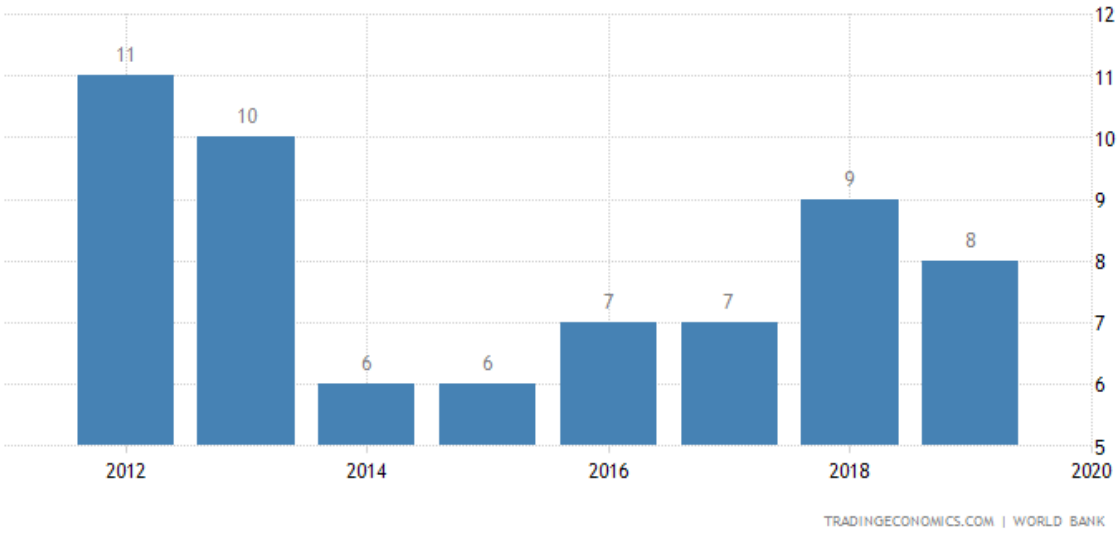
[53] https://www.ipos.gov.sg/resources/for-public-agencies/national-ip-protocol
[54] https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20211231?DocDate=20180312&WholeDoc=1
[55] https://sso.agc.gov.sg/Acts-Supp/9-2018/?ProvIds=Sc2-#Sc2-

4. UNITED KINGDOM

4.1. Snapshot

With a population of 67 million, the UK has played a historically important role in everything technology, research, security and development. It holds a strong position in the financial markets and as a result is always in the financial spotlight. With strong cooperation since WW2, and being a member of NATO, the UK has traditionally been overshadowed by the US and more recently by Israel when it comes to Cybersecurity, defence and technology readiness. While this is not surprising, the UK has ceased to be an imperial power after WW2, instead focusing on a more Europe and NATO collaboration, to boost and maintain its technical capability.

The UK has impressive numbers. It was ranked 8th for the ease of doing business in 2021[56] and has consistently been in the top 15 out of 190 countries over the past 10 years.
The gross domestic product of the British economy was 2.2 trillion British pounds in 2021 and was the fifth-largest global economy, behind the United States, China, Japan, and Germany.



Based on the Global Innovation Index 2021 (GII) the UK ranked 4th out of 1323 countries in 2021 and has stayed in the top 5 over the past 3 years. In addition, the UK also ranks 4th in the 51 high income group economies[57].

From a startup perspective, the UKs 48 unicorns and 40,000+ startups get the most funding, close the most deals and get the most exits across Europe[58]. The UK's ecosystem value jumped nearly 50% in 2021 and approached $1tn. It was ranked fourth globally for VC investments. 20

[56] https://tradingeconomics.com/united-kingdom/ease-of-doing-business
[57] https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2021/gb.pdf
[58] https://sifted.eu/rankings/uk-startups-top-rankings

new unicorns were minted in 2021, more than any single previous year[59]. This is as much as Germany, France and Sweden combined and is third worldwide according to Dealroom. The UK was also one of seven IP offices that received more IP applications in 2021 than in 2022.

Based on our phase 1 report, the UK was chosen as a research target mainly due to the positive intersection of startup and infosec ecosystems. The UK ecosystem has managed to foster and develop both quite independently, and only in the past 7-8 years managed to interlink the startup and cybersec space. This was driven by the need to not lag behind and to continuously attract talent and cybersec technology business to the country. In 2021, there were over 1400 cybersecurity firms operating in the UK, of which over 50% can be identified as micro or small. This 1400+ number has been a 21% increase over the year before and has resulted in startups setting up in the region, companies switching from IT to cybersecurity and new cybersecurity markets being developed with SME/SMBs warranting technology and services

If we include adjacent industries like Regtech and Fintech, the number of operating businesses relevant to security swells to over 8000. And while exact numbers fluctuate on a daily basis, it shows how the UK has been considered to be a magnet for cybersecurity and related technologies. In addition more than 50% are considered to be service providers and 30% focusing on product. The rest are mainly MSPs. 21% of these firms have some international presence which is a great example of how neary one quarter of the business look at international markets to grow as well. Interestingly enough, over 250 international companies have presence in the UK as well. In 2021, the cybersecurity sectors contribution to the economy has been estimated to be $11bn and growing[60].

The National Cyber Security Index (NCSI) ranks the UK 22nd in the global 2021 report. The UK loses out of baseline ICT cybersecurity indicators and in incident response and crisis management indicators[61]. This creates an opportunity for the UK. In comparison, Estonia ranks 5th overall.

All of this is supported by various cybersecurity and startup innovation invitations by the government.

4.2. Government initiatives by the UK

In the UK, the government has help and support for ‘Small businesses’ and additionally startups in some instances. Startups can be classified as both and can take advantage of both

[59] https://startupgenome.com/ecosystems/london
[60] https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2022
[61] https://ncsi.ega.ee/country/gb/?pdfReport=1

opportunities though sometimes there might be restrictions. Some of the organisations and activities are listed below.

GCHQ- Government **C**ommunications **H**ead**Q**uarters or GCHQ is originally an intelligence agency responsible for digital intelligence, information assurance to the government and the armed forces of the UK. It has a historical affinity to code breaking, cryptography, and information warfare as it was originally established after the first world war as the **G**overnment **C**ode and **C**ypher **S**chool (GC&CS). It was later renamed GCHQ in 1946. GCHQ has two components, the **C**omposite **S**ignals **O**rganisation (CSO) which is responsible for gathering information from endpoints and the **N**ational **C**yber **S**ecurity **C**entre (NCSC) which is responsible for securing the UK's own communications.

In 2016, GCHQ launched a joint cybersecurity startup accelerator with Wayra UK, part of the Telefonica group. The accelerator was touted as a game changer as it was one of the first public initiatives by the GCHQ to actively monitor and work with startups. The program ran for 3 cohorts after which it went on hiatus. GCHQ has since started collaborating with HOST (Home of Skills and Technology) and launched a Co-lab which focuses on

1. Dealing with uncertainty
2. Re-imagining morse code
3. Wild card option

This confirms GCHQs position in actively working with entrepreneurs and small businesses.

Department for Digital, Culture, Media and Sport (**DCMS**) is a department of the United Kingdom government, with responsibility for culture and sport in England, the building of a digital economy, and some aspects of the media throughout the UK, such as broadcasting and the Internet. DCMS has a wide scope in different verticals, but has been the premier UK government entity since its formation in 2017, promoting and stimulating the technology and startup sector. From special schemes to targeted funding, the DCMS has a variety of mechanisms by which it tries to boost innovation and development.

Further, DCMS has also supported initiatives that are tailored towards companies that are demonstrating innovation in the field of culture, arts and science. It is also responsible for promoting and supporting cyber security research and innovation and works quite closely with the National Cyber Security Centre (NCSC) to help businesses.

In order to support early-stage ideas and start-ups, DCMS has funded three key initiatives, namely:

- **HutZero**: HutZero is a collaboration between Cylon and Centre for Secure Information Technologies (CSIT) (Queen's University Belfast), It offers a three-month programme designed to help entrepreneurs at the start of their journey. The programme starts

with a five-day bootcamp to develop team working skills as well as business and technical knowledge. HutZero staff are then available to participants for advice and support for the remainder of the programme. Over the last three years, HutZero has supported almost one hundred individuals, and helped to create ten new registered companies within the cyber security ecosystem.

- **Cyber Security Academic Start-Up Accelerator Programme** (CyberASAP): Innovate UK & Knowledge Transfer Network collaborate to help academics in UK universities commercialise their cyber security ideas. They offer a year-long programme divided into three phases: the first focused on developing a value proposition, the second on market validation of the proposition and the third on development of a Minimum Viable Product (MVP) to be presented to funders and industry representatives.
- **Cyber 101:** Delivered in a partnership between the Digital Catapult, The Accelerator Network, Centre for Secure Information Technologies (CSIT) (Queen's University Belfast) and Inogesis[62]. Cyber 101 offers a three-stage series of face-to-face events known as Bootcamps, Deep Dives and Demo-days. They provide expert advice and industry representatives to support the development of critical business skills, contacts and commercial opportunities. It has supported over 160 businesses within the last three years and works across various regions.

National Cyber Force

The NCF was formed in 2018 and is responsible for consolidating and preparing the offensive cyber capabilities of the UK and is jointly set up by the UK MoD and the GCHQ. It operates alongside the NCSC which is responsible for the cyber defensive activities. The unit is relatively new and has an increasingly important role. It remains to be seen if the unit operates standalone, or its scope and command is increased with the increase of importance of cyber offensive capabilities. It should also be known that most cyber offensive activities happen below the radar as compared to cyber defence.

Joint Threat Research Intelligence Group (JTRIG)

The JTRIG unit of GCHQ has remained unknown for most of its existence and was only revealed to the world due to the Edward Snowden leaks. JTRIG's mission includes using all available digital manipulation and offensive techniques to disrupt enemy communications.It is reported that in 2011, JTRIG conducted several denial of service (DoS) attacks on activist group Anonymous[63]. The UK government has also used JTRIG in information warfare against the Taliban[64]. While there is no current role that JTRIG plays with startups, at least publicly, there is a possibility that this might happen in the future.

[62] http://www.ipsos-mori.com

[63] https://www.bbc.com/news/technology-26049448

[64] https://www.nbcnews.com/news/investigations/snowden-docs-british-spies-used-sex-dirty-tricks-n23091

National Cyber Security Centre (NCSC)

The NCSC is the Uk's authority on cybersecurity and policy. Acting as a GCHQ unit, it absorbed and replaced the CESG as well as the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber related responsibilities of the Centre for the Protection of National Infrastructure (CPNI)[65]. The NSCS works with the public sector, private sector and in cases with startups on how to avoid cyber threats. It was formed in 2016 and handles nearly $2.5B of budget on an annual basis.

NCSC has a NCSC for startups program which encourages startups with an MVP to apply to gain access to NCSC technical know-how. The program is based in the NCSC/GCHQ offices in Cheltenham. The program in its current edition is run by Plexal in partnership with Deloitte, CyNam, Hub8 and QA. Only UK registered startups are eligible and all founders and employees need to pass required government security checks. No IP or equity is transferred. NCSC releases challenges every year on its website and encourages startups to apply for the program on the basis of solving such challenges at scale.

London Office for Rapid Cybersecurity Advancement (LORCA)

LORCA is another initiative funded by the Department of Digital, Culture, Media and Sport (DCMS). It is delivered and promoted by Plexal and is supported by Deloitte and the Centre for Secure Information Technologies. It brings together startups, industry leaders, cyber innovators, academics and investors in order to

- Maximise the commercial potential of cyber solutions industry
- Make the internet safer for everyone
- Make the UK a global leader in cybersecurity innovation
- Act as a landing pad and a launch pad for innovators while strengthening the UK's ties with international cyber ecosystems

LORCA runs accelerators and scale up programs in addition to industry forums and lighter programs. They have run five such cohorts of their Ignite program, focusing on scale ups. They don't take any IP ownership or equity. They don't actively invest in the startups they accelerate either. However, startups raise capital based on the network and mentoring provided by the program. The survival or success rate of the startups is currently unknown.

CyLon (Cyber London)

Launched in 2015, CyLon was one of the first cybersecurity vertical focused accelerators in Europe, and the UK. Their earlier stage 'Spark' programmes have supported hundreds of cybersec entrepreneurs. Their equity for investment program paved the way for the first true UK based ecosystem developer. Since the UK, CyLon has launched high profile programmes in Singapore, where it provided a similarly structured program and frequently supported cross

[65] https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

pollination. As both the UK and Singapore were entrepreneur friendly countries, startups were able to benefit from such a large ecosystem. Since Singapore, CyLon now operates in over 35 countries, though not all countries are regular and cannot be considered regular programs.

Since their Spark programs, the CyLon product offering has increased to scale ups, via its Cylon Scale program. In addition, realising there is a need to help underrepresented communities entering the cyber field, their Go program works towards bringing more diversity in the cyber vertical.

Enterprise schemes

The UK government has four different types of schemes to help startups and enterprises grow. Of these the Enterprise Investment Scheme (EIS) and the Seed Enterprise Investment Scheme (SIES) seem to be the ones that are focused more towards startups in the early stage of development.

The Enterprise Investment Scheme is targeted to later stage companies and is only available for companies with no more than 15 million in gross assets and with less than 750 employees and a company which is not older than 7 years.

The Seed Enterprise Investment Scheme is for younger companies for companies that are less than 2 years old at the time of investment and don't have more than 200000 in gross assets with less than 25 employees. The other two schemes, the Social Investment Tax relief scheme and the Venture Capital Trust schemes are both for companies as well, however in our interviews none of the startups spoke about these schemes, however they are worthy of attention.

The Seed Enterprise Investment Scheme (SEIS) has been a boon for startups trying to raise money recently and is one of the key schemes that most founders mentioned in their interviews. This scheme is designed for even earlier stage companies than the Enterprise Investment Scheme (EIS) participants.

The Seed Enterprise Investment Scheme startups can accept up to £150,000 from SEIS investors. Early stage investors are given tax relief of up to 50% of the investment which adds up to significant capital gains and losses reliefs. There are very specific requirements that the HMRC has set for companies to qualify and can be viewed at https://www.gov.uk/guidance/venture-capital-schemes-apply-to-use-the-seed-enterprise-investment-scheme.

Under the EIS scheme, a company can raise up to 5 million pounds each year and a maximum of 12 million in its lifetime. The company must also use the money for its own growth and development. More information about this scheme can be found at https://www.gov.uk/guidance/venture-capital-schemes-apply-for-the-enterprise-investment-scheme

Interviewed founders found the SEIS and EIS schemes extremely useful, relatively lightweight to implement and very important for the early stage investment needs. It also enabled

founders to raise capital from their home countries and at a later stage attract international capital without worrying about exhausting financial runway.

We feel the similar strategy in Estonia could make sense even though its current investors are far more international and open to invest in considering or combination of such a scheme with assistance to hire talent by the government would be a step in the right direction.

5. INTERVIEW INSIGHTS

Interviews and insights from Cybersecurity founders and ecosystem players from the UK and Singapore. As part of this proposal, Startup Wise Guys conducted semi-structured interviews with founders from different stages of the startup space, advisors and ecosystem players and some of the insights that were received were used to develop the strategy for Estonia. Total six interviews were conducted and all respondents wished to remain anonymous. We note that four purported respondents explicitly declined the interview when we explained that it is part of a study for a government. Furthermore, despite our outreach to dozens of potential interviewees in both Singapore, the UK and beyond, the response rate remained very low. The insights are summarised according to the opportunities and questions asked (Questionnaire can be found in the Annex).

5.1. Start of their journey

As founders, most founders we spoke to started because of a mix of all the right ingredients at the right time. Whether it was an idea they had developed for a couple of years in their head, or something that came to them due to existing market conditions, most did not require any early stage ideation to get them going. This was also because the majority of the founders we spoke to were more mature with either corporate experience under their belts or with a further degree program. This made us question the relevance of early stage pre-idea development programs, and while none of the founders had taken advantage of such programs, they were quite optimistic that such programs would help develop the ecosystem.

Another interesting topic was co-founders and the ability to find good co-founders. One respondent joined a venture builder to try and find a cofounder, but in the end had to find them externally. A good insight on this topic was the nationality and build up of the team. A lot of teams we spoke to were made up of international co-founders rather than founders from just one country.

5.2. Government assistance

We also asked respondents in our interviews on the role government ministries or entities played in their trajectory and journey. Most agreed that direct government help was not forthcoming, and that was okay for them. Even though both the UK and Singapore have simple to navigate ecosystems, founders mentioned that government assistance via other third parties was the best way forward. They also mentioned that if this was easier and with less red tape, startups would benefit more than if they had assistance as they do with EU project based funding currently, which has a huge application and reporting overhead.

Most also agreed that government grants were a good thing for very early stage development, but founders did not find the lack of grants at later stages an issue. They did encourage the government to invest more capital, but via existing vehicles like Venture Capital or similar investments rather than grants at a later stage. This would enable them to stay relevant and attract both strategic and financial investors. Grant money at later stages, unless used for R&D purposes, is extremely difficult to follow up on, and most investors like to know how this money was used. At this point it is also important to mention the UK government's R&D tax relief scheme which UK founders spoke highly about. While not as easy to apply for as it could be, founders found this scheme highly valuable at the point where they need a larger jump from their version 1 product, to a more sophisticated product which then provides a higher value to customers and indirectly increases the valuation of the company. A couple of founders also felt the various loan schemes set up during the COVID pandemic had a positive impact on cash flow for them, and encouraged more such guaranteed backed loans to be made available even outside the emergency situations.

One noteworthy mention here was also the government's initiative with helping startups at trade shows. Founders found this particular initiative valuable in creating international and local hype within the ecosystem, and in the long term helping with creating an international network. Founders also said that they would not have chosen to apply for trade shows or international show booth spots if it weren't for national pavilions and the government's initiative to take upcoming startups there.

5.3. Ecosystem assistance and impact

We also explored the overall ecosystem elements that assisted positively or negatively the trajectory of cybersecurity and dual-use startups in the two focus countries. One thing was quite evident from the start is that founders had attended at least one if not two or more accelerator programs. Though none had attended two cash for equity programs, due to the negative effect two such programs back to back have on the cap table, most had attended at least one program either by CyLon, Antler or Cyrise. In addition, they had also taken part in non-equity accelerators which are focused around mentoring and light industry access. Founders commended such programs, but mentioned that two elements were completely missing. Technical know-how training and guidance was missing from nearly all the accelerators and was a much needed piece of the startup toolkit. Some founders had to go to

the US or other ecosystems to get that technical know how from more experienced founders. One such respondent went to live in a hacker house in the US for weeks to try and get more access to the cybersecurity technical world. The second thing that was flagged up was the low level of peer learning in the programs. Whether this was due to the fact that there were not enough mature founders or the fact that the vertical itself is more competitive was not known.

5.4. Elements missing from the ecosystem

Interviewed candidates had one major requirement of the ecosystem which was currently unfulfilled. The ability to access customers via a curated process. Most startups are new in the market, and as defence and cybersecurity are industries of trust, startups found the ecosystems lacked initiatives where close quarter interactions with customers was possible. They also found the sales cycles really long and felt such initiatives could reduce sales cycles, reduce runway requirements and generate revenue early. A few of the strategies in this report focus on trying to facilitate such a process, whether it is via a face to face event or an online marketplace/platform.

6. ANALYSIS AND PROPOSALS

Based on the above models and information provided during interviews, this chapter outlines elements of a potential solution for creating an Estonian defence sector and dual-use (start-up) ecosystem. First, we identify broader principles, which we distilled from observing common elements in the studied models, dynamics, ongoing processes and new developments related to this field. Second, we propose strategies to address the various aspects of the ecosystem to be created. We also aim to propose a model that can lay the foundations for a self-sufficient ecosystem in the longer run. Roles for ecosystem players are proposed throughout the following subsections.

6.1. Underlying principles

The selection of Singapore and the UK for analysis were based on their well-known success in creating cybersecurity startup ecosystems and their comparability to Estonia in terms of size and digitalization. However, it should be noted that there are several differences between these countries in terms of their integration in the global startup ecosystem and their approach towards the role of the state therein. Both the UK and Singapore feature a vibrant startup ecosystem and relative ease to venture capital, while Estonia receives comparatively modest attention globally in this respect. Another key difference is Singapore's strong interventionist policy and its significant means channelled into driving growth. Due to these

factors, the examples created by Singapore and the UK should be regarded with caution and not to be used as a one-size-fits-all formula. However, there are plenty of elements in each analysed ecosystem that provide interesting opportunities and may be considered to be adopted in creating the Estonian defence and dual-use startup ecosystem.

Based on the above, key ingredients in the form of underlying principles can be identified. Working with these principles, rather than always directly with the particular practices and experiences in the examined ecosystems, allows us to take a broader perspective and tailor our proposals to the local context of Estonia.

A. Co-creation and strong collaborative ties - It is most noticeable in Singapore that grants, fellowships and general support measures, are most often tied to the criteria that there should be an industry partner, so that the innovation process progresses towards real-life needs. Industry partners are also expected to contribute and interact with other ecosystem stakeholders in all phases of startup growth. UK's GCHQ's and DCMS initiatives also confirm the importance of this principle.
B. Outward-looking and accessible development - Both Singapore and UK ecosystems have significant externally facing traits. Given Estonia's small market, it is imperative to remain focussed on the external environment and ensure that no segmentation would take place based on nationality, place of incorporation, etc. However, Singapore interviews hinted that the requirement to be linked locally is a hurdle in accessing programmes. While Estonia's e-residency schemes make the local institutional system highly accessible, attention also should be paid to possible gaps.
C. Sharing (of targets, roadmap, responsibilities, spaces, resources, tools, processes, benefits, ecosystems, etc.) - Ecosystems are composed of its elements and the synergy inbetween. Only by sharing 'things' and making them visible, available and known about can those become 'common'. Otherwise the same will be repeatedly reinvented and duplicated over time. A good example for such sharing is the linking of R&D and testing infrastructure with accelerators in Singapore.
D. Commitment - Commitments should be both realistic and aligned with ecosystem goals. Commitments should be sought both at organisational as well as individual levels from participants. Commitment is evidenced by the visibility of engagement of public agencies in the ecosystems both in Singapore and the UK.
E. Sustainability and long term view - Defence sector innovation and market success is characterised by long cycles compared to other sectors. Insight from Singapore's Cape Vista CEO is worth considering, who pointed out that making money like a typical fund is not a primary goal, but to get the technology to put to use in the ministry, armed forces, or the government agencies and to trigger investor interest is a competing priority. The ecosystem setup should allow for long incubation periods and take into account the high market entry barriers.
F. Human-centric approach - Team is key and teams are composed of individuals. Team setup, team building support, measuring team ability, and syncing team and innovation development should be a focal point in the ecosystem. Some of the studied solutions for example required that teams should have a business/development person (or a mentor) in order the proposal to be eligible for the programme.

Furthermore, attention should be paid to individual (self-)development and wellbeing from a holistic perspective.

G. Green and gender-conscious approach - Both green and gender policies of the EU are now cross cutting and keeping in mind these priorities in creating and developing the cyber/defence ecosystem would add a unique touch to the Estonian solution. We have not encountered any cyber/defence ecosystem that would explicitly focus on these areas, thus this could distinguish the Estonian approach at the global scene. It would not only be in line with EU priorities, make participation a reputable affair demonstrating high corporate social responsibility, but potentially open further financing opportunities for the development of the ecosystem.

6.2. Strategies

While there is no single correct or complete solution, there are a collection of activities and strategies that can help Estonia's cyber/defence sector create a progressive and profitable ecosystem. Let us look at some of these strategies in details.

6.2.1. OPERATIONAL STRATEGY

This involves setting up an entity or unit 'CollaX' that forms the interface between the public and government bodies and the ecosystem from an operational perspective. This is extremely important and in our interviews was highlighted as one of the more difficult strategies to achieve. CollaX is the operator of the ecosystem.

The speed at which the private sector or the entrepreneur space works is not aligned with the slower pace of the public sector. The regulations, procurement and risk appetite of the public sector is something that entrepreneurs seem to underestimate or spend a lot of time trying to overcome.

In Singapore the Cybersecurity Consortium fulfils the role of one similar interface, however it is anchored in the entrepreneurship-oriented wings of academic institutions, which 'co-operates' the ecosystem. In the UK the NCSC has recently tried to take on such a role, but due to its association with GCHQ has had to look at private entities to take this role on. And here-in lies the first problem, as private entities are considered service providers in this role and have no upside to the success of the sector.

Therefore, the right strategy for Estonia would be to have a light, lean and forward thinking organisation, made up with the ranks of various government ministries and agencies, representatives from universities and a few private highly motivated individuals, answerable to the Ministry of Economics, but operating as an independent entity. This could be a Startup Estonia like setup, but very specifically for defence and security, with members from that vertical. The purpose of this would be

- , Interface with all government ministries, MoD, armed forces etc and the private sector, entrepreneurs and academic institutions
- This unit would communicate the needs and wants of the government entities on a yearly basis to the defence sector and academia
- This unit would then collaborate and work with the private sector of universities, accelerators, ecosystem builders similar to the way the DCMS does in the UK, but on an operational level
- The unit would interface with the technical know-how needed to operate a vertical focused on defence and security. To do this it will need to have good buy in from the various defence entities like the EDF and MoD of Estonia
- The unit would support the other strategies listed in this report

It is not inconceivable that CollaX could be located at the Estonian Defence Industry Association and it could fulfil this role (jointly with a university), since it already reaches out to key stakeholders in the defence sector, has thorough understanding of the sector, has some cyber-specific focus. However currently there appears to be modest or no emphasis on pre-seed, seed and early-stage startups. The Defence Estonia Cluster has already been contemplating to take on new roles, such as being the central coordinator for defence and security foreign investment, organise and administer visits in this field, etc. While tasking the Defence Estonia Cluster with the above would avoid unnecessary duplication, deep integration with the broader startup ecosystem would be desirable. However, if a new entity is set up, the Defence Estonia Cluster would certainly be a key partner.

Ecosystem operator would need to:

- Orchestrate and develop the ecosystem
- Coordinate & support resourcing
- Deploy initiatives
- Implement accessible knowledge exchange
- Manage knowledge repositories and idea portfolios
- Operate and develop digital ecosystem activities
- Manage the streamlining of green and gender policies within the ecosystem

Ecosystem operator entity (CollaX) takes ownership and provides board, composed of representatives from main driver organisations, including:

- MoD
- EDF
- MKM
- RIA
- Estonian Business and Innovation Agency/Startup Estonia
- Universities
- Defence Estonia Cluster

Ecosystem advisory/expert board: a group of internationally renowned experts in the field. In our proposal we emphasise the initial roles of key entities, however this pertains to the role of ecosystem operator and orchestrator. This does not take away from the importance of the roles of entities not mentioned by name so far, such as the Defense League, CR14 Foundation and others. While we do foresee a strong driving role for the ones mentioned under the operational strategy, it is just as important to cultivate strong partnerships with defence-linked organisations.

6.2.2. SECTOR DEVELOPMENT STRATEGY

The objective of this strategy is to develop and build a healthy pipeline of defence and security startups by activating grassroot level sector focused activities.

Currently these are done on an ad hoc level. In our interviews, founders had no access to such activities, so while their success cannot be attributed to the early stage development strategies, they indicated that such activities were missing and could have reduced their startup time if they had existed for them.

We build an early stage pipeline by looking at an n-2yrs horizon and focusing on the defence and cybersecurity vertical. N being the time we expect founders to establish their companies in Estonia. This strategy may be delegated operationally to the existing setup of Startup Estonia with the input and assistance of CollaX above.

Sector development should be targeted to University level and later participants with the sole objective to ideate solutions to problems defined by the government defence entities and driven by the CollaX unit in pt 1 above. CollaX does not screen or reject any ideas or projects

at this stage as the activities work on building both the defence and the startup skills of the participants.

Activities in this strategy include

a. Idea hacks – Activities designed to develop ideas
b. Hackathons
c. Capture the flag and other technical events designed to bring technical know how to the forefront
d. Preaccelerators, online and in person
e. Talks by defence entities to inspire participants to join the sector in solving problems
f. Guest lectures, tutorials, workshops and seminars by international and local researchers capturing defence-related topics
g. Train the trainers activities in the cybersecurity ecosystem
h. Networking and match-making events

One key objective of this strategy is to ensure participants can see the end to end journey of a founder or startup. Thus, we need to connect to accelerators and incubators who will take the output of this strategy and develop them to more serious startups. This is another negative of the existing setup in the UK, where such activities are delegated purely to private players who are then treated as service providers. Besides some KPIs there is no vested interest for the service providers to go above the requirement. Having this public private setup has worked well in Estonia in the past, and with the vertical and customer expertise coming from CollaX, the impact of these activities will be very focused to the defence sector.

Furthermore, Singapore's example showed the importance of co-creation and the alignment between research/ideation and actual market needs. Singaporean universities commercialise great portion of their research, which is likely due to the focus on supporting researchers and scientists with entrepreneurial education programmes (such as the 10 weeks intensive training Lean Launchpad Singapore) as well as strong cooperation between industry, government and entrepreneurial arms of higher education institutions (NUS Enterprise and SingTel are co-founders of ICE71 the cybersecurity innovation hub, CSA supports and Enterprise Singapore finances some activities). Thus Estonia needs to better tap into the resources of the industry and academia in order to create better synergies, responsive, needs-based innovation and building a cyber talent pipeline. While cyber-related competences and also the readiness to create new ones exist in several organisations, there is room for further cooperation across sectors.

Sharing of information and responsibilities appears to be key ingredient in this respect, where priorities should be given to joint activities (e.g. joint (pre-)acceleration programmes; organising student challenges/competitions responding to real industry needs; co-designing

and co-instructing education programmes such as open and regular university courses; tailored train the trainers seminars). It is recommended that modelled on the recent cooperation arrangement between AS SmartCap and University of Tartu to create a research accelerator in the field of health technologies[66], SmartCap/Estonian Business and Innovation Agency could explore the opportunities for establishing a cyber/defence research accelerator.

6.2.3. MARKET ACCESS STRATEGY

The objective is to provide collaborative support in accessing potential markets and preparing for procurement.

One of the biggest asks from our interviews was the ability to get access to the defence and security market. Founders were very clear on how difficult it was to get to customers and nearly no strategy was in place to get them in front of customers, or in helping them navigate the procurement practices of said customers. For startups, time is money and long sales cycles are a death knell for their business. So the objective of this strategy is, again, working in collaboration with CollaX, and other private entities, local banks, Telcos, SMBs, SMEs and collectives like the Estonian Defence Industry Association and Fintech Association of Estonia. The objective is to be able to pitch to and initiate sales cycles with customers without the overhead of lead generation etc. This strategy will also help founders and startups get prepared and equipped for procurement.

Certifications and accreditation advisory and support should also be provided. This has been an important pillar of the Singaporean strategy, going as far as developing local certification and accreditation capabilities. While it may not be cost effective for Estonia to follow suit, there is more that can be achieved by supporting the local testing, inspection and certification industry (e.g. by facilitating access to experimentation, validation, testing resources, such as CR14 Foundation's OCR and other cyber ranges) and building local expertise in this field.

Defence and dual-use technology startups will need advice on how to handle particular import/export controls. This type of assistance is of utmost importance for the sector, since these regulations determine practical viability of solutions and access to markets outside the EU. The hurdle is very high for startups, as the Recast Regulation (EU) 2021/821 on dual-use items introduced novel provisions, in particular related to surveillance technologies, the so-called catch-all provision imposing export controls based on human-rights considerations, the interpretation and application of which is currently still unclear and lacks guidance.

In our interviews founders also found the lack of such a market access strategy, increased their time to find sales leads and also reduced the market insight they were able to collect. It should

[66] https://smartcap.ee/smartcap-greenlights-the-creation-of-a-science-accelerator-for-health-technology-research/?pageNumber=1

be remembered that market access strategy is not only about sales, but is also about providing access to market insights, which is usually via live interactions, interviews and reports.

The strategy can land as either one off events, a physical hub of defence and security with space for people to meet or an online space similar to market place working on simplifying this process.

6.2.4. FUND STRATEGY

Set up an investment fund by AS SmartCap (subsidiary of Estonian Business and Innovation Agency) or a similar entity, to be managed by dedicated private fund manager(s).

Another insight from our interviews was the role of the ecosystem in funding startups. It was clear from the insights that:

a. Startups all raised their first round from angels, but usually via an accelerator which also invested in them;
b. Startups didn't take any government money or grants at a later stage of investing, relying on private/venture capital for that;
c. Government grants were useful, but only before formal capital for equity was raised;
d. Government schemes that assisted in hiring or in R&D tax relief were utilised by startups wherever possible;
e. Schemes like the SIES and EIS which rewarded angel investors and private individuals with tax relief if they invested in startups provided a lot of early capital opportunities to the founders.

The one outcome of the above is the realisation that governments should not manage direct or even fund investments directly into startups. Instead they should entrust the capital to private fund managers, who have their own skin in the game, and have an upside opportunity which would lead them to perform towards everyone's benefits.

An example of such can be seen in neighbouring Lithuania, there for the last 6 years Invega has been awarding funds to private fund managers. The first fund awarded in 2018 in Lithuania made 30+ investments and is currently invested in nearly every top Lithuanian startup to watch. In 2021 INVEGA released a tender for a similar fund but for defence dual use and security. Some features of this strategy are mentioned below and why they may prove to be very useful for Estonia:

a) Fund managers have to raise 10% or more of the fund size as well;

b) Fund managers and fund team have to invest their own capital in the fund as well, ensuring that fund performance directly impacts he fund team. While not indicated it is advised to be between 0.5% to 1% of the total fund
c) INVEGA and the fund of funds contribute a fixed fund capital of Euro 10million
d) As a government entity, INVEGA capped its upside to the hurdle rate proposed by the fund manager. This hurdle rate was suggested at 5-6% per annum keeping in mind annual interest rates and opportunity cost of capital. The interesting element here was that even in the event of a large exit, the fund would only ever accept an upside of the hurdle rate per annum across the INVEGA contribution. This meant that private investors and fund managers would be able to magnify their upside, effectively leveraging their capital. This enabled fund managers to raise capital quickly and also enjoy a multiplier on exits.
e) The total capital in the fund was to be used for early stage, pre-idea and seed investments, effectively giving the whole fund visibility of the end to end pipeline. It also meant, to have a successful fund, fund managers had to also focus on pre idea and early stage activities. Activities that are a part of the sector development strategy

It remains to be seen how this fund performs on maturity, but going by indicators, it has achieved a few things for Lithuania:

i. Kick started private investing in the country

ii. Increased the visibility of the ecosystem to private players now that there are more than ever investible startups

iii. Helped prospective founders get inspired by the success stories and push themselves into Entrepreneurship

iv. Inadvertently created a more balanced and supporting investing ecosystem across the Baltics, with only Latvia lagging behind in sheer numbers.

Estonia has been using a similar construct since 2011 and AS SmartCap, the tech-investment arm of the Estonian Business and Innovation Agency, and manages SmartCap Venture Capital Fund and SmartCap Green Fund, both being venture capital fund-of-funds, and its portfolio boast unicorns like Bolt and Veriff. SmartCap's activities have been self-sustaining, but it does not have a specific defence/DU/security fund.

This report also revealed that with some variations, similar constructs have been used by Singapore (Cap Vista Pte Ltd, Enterprise Development Board Investment which manages the fund-of-funds modality under Startup SG Equity) and the UK.

We feel that INVEGA's strategy combined with SmartCap's approach has a huge upside potential for the defence ecosystem in Estonia and while there might be a few modifications and alterations to the overall setup, having the ability to deploy large sums of capital, rather

than capital one by one by the government can really accelerate the ecosystem and get startups more confident about the funding side of their startup.

The key here is the ability to simplify and unify the access of state capital for the ones who need it, by letting entities who know how best to provide the capital provide it, all in one go, rather than one by one. AS SmartCap's credentials, reinforced by similar practices in other countries, leave little to doubt that a cyber/defence oriented fund could follow the pattern of previous successes.

Some additional elements that might help this strategy would be to create annual audits and freedom for the investment committee to invest as long as the investments are made in Estonian registered and tax contributing organisations. The key here is to make Estonia the destination for defence startups, with simple and equal opportunity to investment.

6.2.5. INTERNATIONAL STRATEGY

The International strategy is required to make access to market, capital, talent and attract the vertical to Estonia.

This is important because unlike other countries like USA, Israel, Germany or the UK, Estonia as a market is not sufficient for startups to thrive. And which the defence and security sector is a closely guarded vertical, Estonia needs to have a strategy to keep it closely guarded yet be able to make it profitable in the long run for the startups. This push pull strategy is required as we want startups and the sector to have long term stickiness. In our interviews, participants only opened entities in other jurisdictions due to complex issues in their home jurisdiction or get access to later stage capital. This may be avoided if the international players have full confidence in the Estonian market. And to do this, specially from the US requires extra effort and a conscious effort.

The international strategy will be focused on two elements.

i. Investments and capital
ii. Market access commercial and technology

i. Investment and Capital – This is the key for startups to survive and not die. While the fund strategy shields the vertical from variations here, investors are often pack individuals. They like to co-invest and will often look at markets other than their home market to diversify if possible. For Estonia's success in the defence and security vertical, there needs to be a constant flow of investors to the country. At least once a quarter, a conference, meetup summit or private showcase of some kind specifically designed for this vertical is suggested. While we have events like Startup Day and Latitude 59, these are too startup generic and serious defence investors stay away. On the other extreme, events like Lock Shields and events

hosted by the MoD are too defence oriented and have no visibility to the investor community and therefore are missed out. A halfway type of event every quarter, in association with entities like the European Cyber Security Organisation (ECSO) and CollaX from pt1 above could help create the international environment needed by this vertical

ii. Market Access and technology - While there are a lot of ways to achieve this, our interviews with founders suggested two interesting strategies. Founders were extremely positive about the opportunity to go visit other markets via home nation pavilions at exhibitions abroad. Nearly every founder we interviewed said they were supportive of this opportunity. They also mentioned that this gave them access into markets they would otherwise have a hurdle entering. However, in such cases they were at the mercy of the exhibition or conference type. We aim to eliminate this.

While there is a lot that needs to be done to develop market access for startups in Estonia itself, creating collaboration bridges with friendly countries in the NATO and abroad could open markets not available to founders. NATO countries aside, countries like Australia, Singapore, the Nordics and the US are all open to cross border trade in the defence and security vertical, with Singapore and Australia especially receptive as they try to build their own ecosystems. Creating 1-2 week soft landing missions focused solely on meeting market players in other countries and understanding technology acceptance level, along with the understanding of competitive landscape in other markets would help the vertical shorten time to international expansion. Doing and receiving such soft landings would help build the international bridges the vertical needs.

Furthermore, links should be established and cooperation should be sought with other similar ecosystems, some of which have already been established (CyLon, ICE71) or are currently being developed such as shown by the above INVEGA call in Lithuania, or the Cyber Academia and Innovation Hub (EU CAIH - a PESCO project) in Portugal.

6.2.6. TECHNOLOGY STRATEGY

The technology strategy is ultimately needed to make sure access to technology, technical know-how and technical problems to solve is available to the startups and the vertical. And this is where the vibrant university, labs and research sector of Estonia comes into play.

However, there is more that can be done.

i. Promote companies, especially small and medium companies, startups tapping into this resource - To achieve this, Estonia can look at successful schemes internationally. However the UK has been running a scheme designed specifically to assist SMBs with technology transfer. The

Knowledge Transfer Partnership is a scheme that enables SMBs tap into the technology being developed by the University or research organisation, and creates a temporary hire position which facilitates this transfer majorly funded by a government entity. Both SMBs and the University whose technology is being transferred also invest time effort and a modest financial contribution, and have skin in the game. This scheme is successful as it also gives the startup/SMB the ability to hire someone for a limited 1-2year period, and then subsequently offer them direct and full employment. The Associates hired to do this technology transfer end up with service/product management/development roles, which are one of the most difficult profiles to hire early on.

ii. Accessing technology partnerships internationally – This is a little more complicated and longer term to achieve. However it is imperative that universities collaborate and publicise this on very specific defence/security vertical topics. We are aware of such collaborations however publicising this not for the student market but for the founder/startup market is key. There also has to be a process by which technology demands of the MoD or vertical can be conveyed to the startup ecosystem in a timely and unified way. This is again something that CollaX from point 1 can drive.

6.3. Options and models for co-financing the ecosystem

In (co-)financing the ecosystem there are currently several unknown factors due to the ongoing processes in the EU regarding ESIF and EDA fundings. However, these two seem to be key sources for public sector contributions, unless Estonia decides to solely fund proposed activities. Furthermore recent developments in NATO show promises as to future useful resources.

6.3.1. ERDF

The Startup Estonia programme, also SmarCap and KredeX efforts reach back to the European Regional Development Fund (ERDF). The new text for the regulation of the European Regional Development Fund and on the Cohesion Fund[67] indicates that innovation and smart economy will remain as a priority, however in the absence of an operational decision, the practical details cannot yet be seen. During the consultations for determining priorities, the keywords of defence and security, dual-use, cybersecurity, startups and

[67] Regulation (EU) 2021/1058 of the European Parliament and of the Council of 24 June 2021 on the European Regional Development Fund and on the Cohesion Fund

innovation were used and discussed, yet most of the previous periods' ERDF funds appear closed, and new ones not yet opened. However, based on previous practice and successes, it is likely that European Structural and Investment Funds will offer suitable funding schemes to set-up and also to operate the ecosystem.

6.3.2. InvestEU

Besides the already known go-to source of ERDF, better visibility is currently provided on the InvestEU programme. The InvestEU is the defence equity facility established as the implementation of the EDF. The European Investment Bank, implementing partner of the InvestEU programme, has published several calls for expression of interest in April 2022, which may be considered to co-fund the cyber/defence startup ecosystem. Particularly promising call and appears compatible with the strategy recommended herein, is the InvestEU Equity programme, which aims at selecting eligible financial intermediaries under the framework of InvestEU for providing equity investments in support of innovation, growth and social impact.[68] Under InvestEU Equity, the EIF will provide equity investments and co-investments to, or alongside, funds in the areas of venture capital, private equity and private credit, that pursue generalist, specialised or mixed investment strategies. Under InvestEU Equity, the EIF will make investments into or alongside financial intermediaries. The two thematic strategies within which the investments will be made are the 'Enabling Sectors' and 'Digital and Cultural & Creative Sectors'. The first explicitly includes the defence sector and aims to sustain the technological sovereignty of the EU by investing in deep tech, critical industries with a significant R&I base tackling unmet medical needs, securing semiconductor and/or hardware production and supply as part of the Chips Act, strengthening the defence & security base of the EU, and accelerating and maturing the upstream and downstream space sector in partnership with the CASSINI initiative, part of the European Space Programme.[69] The latter explicitly includes cybersecurity and contributes to strengthening the EU's digital independence and strategic autonomy with investments focusing on data, communication technologies, services and products that facilitate digital transition. Particular focus will go towards digital technologies central to the Digital Europe Programme (such as artificial intelligence, blockchain, quantum technologies).[70] Horizontal priorities, which applicants must consider include gender criteria, and adherence to European various initiatives related to investment strategies. The size of InvestEU investment is up to 100MEUR, up to 25% of the total commitment of the financial intermediary. The call is open until 30th June 2027.

[68] https://www.eif.org/InvestEU/equity_products_calls/index.htm

[69] EIF Open Call for Expression of Interest to Select Financial Intermediaries - Supporting risk capital for innovation, growth and social impact investments in Europe. Published on 13.04.2022.

[70] Ibid.

6.3.3. EDF

Furthermore, promising opportunities are envisaged by the European Defence Fund, although some of its programmes are expected in the coming months and years. The 18.05.2022 Joint Communication on the Defence Investment Gaps Analysis and Way Forward focuses on various aspects of enhancing EIB's support to defence, expects EIB to expand investments towards interested promoters and partners the support of R&T cooperative projects, and work with promoters in the early phases of their product development. As a concrete action to be expected, the Commission will propose by the third quarter of 2022 a European Defence Investment Regulation defining the conditions and criteria to form European Defence Capability Consortia, as a basis for VAT exemption for joint procurement and a vehicle (including possible co-funding) for European defence projects of high common interest. Essentially a joint European Defence Investment Programme will be proposed by the end of this year.

6.3.4. HEDI

It should be noted that the EDA just recently launched the Hub for EU Defence Innovation (HEDI), which will serve as a platform to stimulate and facilitate cooperation on defence innovation among Member States while ensuring synergies with related European Commission activities, notably the EU defence innovation scheme, and coherence of output with NATO innovation initiatives. HEDI's initial portfolio will be organised in 6 clusters, common picture, EDA innovation prizes, innovation challenges, proof of concept/demonstrations, European Defence Innovation Shows, uptake of innovation, all of which imply the availability of important resources and opportunities for the Estonian ecosystem. Hence, it is recommended to rely on and synergize HEDI's tools with the local ecosystem, in order to avoid duplications, and optimise resourcing and financing.

6.3.5. NATO DIANA

Another key initiative, with which synergies should be sought is NATO's Defence Innovation Accelerator for the North Atlantic (DIANA).[71] While DIANA, which is meant to be similar to US's DARPA, is in its initial stage, it will run 10 accelerator sites and over 50 test centers, and it promises a 1 Billion EUR venture capital for early stage startups. Since Estonia and UK were announced as the hosts of DIANA in Europe, it is imperative that the Estonian cyber/defence ecosystem is aligned with the commitments already taken with the DIANA bid.

[71] https://www.nato.int/cps/en/natohq/news_194587.htm

6.4. Select legal aspects - state aid and intellectual property rights

In overall, since the proposed construct is not expected to bring about significant novel features that would create a previously unknown situation or conflict with current legislation, it can be stated that the authors of this report do not foresee the need for any significant changes in current legal frameworks. Moreover, even if changes in the relevant legal frameworks may not be a local affair, since the regulatory frameworks in these respects are predominantly based on EU and international rules. At the current stage of analysis it appears that state support can be designed within the framework of state aid rules and management of intellectual property (IP) protection is the question of contractual arrangements.

However, this does not mean the lack of legal risks or considerations. Therefore, this chapter is divided into two main parts and corresponding discussions: Firstly, we address overall (selected) legal challenges and risks with the creation of the proposed ecosystem. Secondly, we point to some legal considerations for potential use cases arising from the ecosystem.

6.4.1. State Aid

The setup, operation and development of the cyber/defence ecosystem along the lines recommended in this report may involve measures that qualify as state aid. Article 107 of the Treaty prohibits state aid unless exceptionally justified. State aid includes subsidies, grants, guarantees, government holdings of a company, tax reliefs, providing goods or services on preferential terms, etc., so measures recommended by this report needs case-by-case assessment.

Since the measures recommended in the Estonian cyber/defence ecosystem are mainly aimed at pre-seed, seed and early-stage startups, as well as research and development, there is a likelihood that exceptions may apply.

The use by the state of InvestEU Equity, ESDF, EIB/EDA, NATO and other funding for supporting cyber/defence companies can be state aid if there has been

- granting assistance by state or through state resources;
- favouring certain undertakings (an advantage);
- selectivity;
- distorting or threatening to distort competition and affecting trade between Member States.

European Structural and Investment Funds (InvestEU, ESDF, EIB resources, ect) are considered State resources as the national government influences the way they are spent. State resources are all the resources of the public sector[72], which can also include resources from NATO.

[72] Case T-358/94 Air France v Commission [1996] ECR-II-2109, para 56.

Advantage is understood as an improvement in market position of an undertaking due to co-financing of its activity. State measure which favours certain undertakings or the production of certain goods, types of undertakings, sectors or regions is selective. Furthermore, if the measure improves the competitive position of the recipient and also affects cross-border trade, it may also be prohibited. Grants, cash for equity programmes, financing of training, aid to export-related activities are all such that they are likely to improve the market and competitive position of the recipient, and are also selective.

Nevertheless, due the context, activities and beneficiaries of the proposed ecosystem, various exemptions may apply, thus regardless that a measure qualifies as state aid, it may be compatible with the internal market and thus be allowed. Such exemptions for aid schemes include in the various forms mentioned several times in this report:

Aid to SMEs (Articles 17-20 of GBER[73]):

- Investment aid to SMEs, investment in tangible or intangible assets related to formation of companies, expansion of companies, etc.;
- Aid for consultancy in favor of SMEs, except for routine consultancy services (such as tax, accountancy, legal);
- Aid to SMEs for participation in fairs.

Aid for access to finance SMEs (Articles 21-24 of GBER)

- Risk finance aid, such as equity or quasi-equity, or financial endowment to provide risk finance investments directly or indirectly to eligible undertakings; Loans and guarantees, tax incentives;
- Aid for start-ups, meaning aid for enterprises less than 5 years old and the form of aid can be loans, guarantees, grants, equity or quasi-equity investments
- Aid for scouting costs

Aid for research and development and innovation (Articles 25-30 of GBER):

- Aid for research and development projects, including (a) fundamental research; (b) industrial research; (c) experimental development; (d) feasibility studies.
- Investment aid for research infrastructures;
- Aid for innovation clusters;
- Innovation aid for SMEs, such as a) costs for obtaining, validating and defending patents and other intangible assets; b) costs for secondment of highly qualified personnel from a research and knowledge-dissemination organization or a large enterprise, working on research, development and innovation activities in a newly created function within the beneficiary and not replacing other personnel; c) costs for innovation advisory and support services;

Training aid (Articles 31 of GBER)

[73] COMMISSION REGULATION (EU) No 651/2014 of 17 June 2014 declaring certain categories of aid compatible with the internal market in application of Articles 107 and 108 of the Treaty

The above schemes clearly relate to activities and elements that are typical and essential in a startup ecosystem. The accelerators, funding schemes, support services, research activities, development and access to infrastructures, acquisition of tangible and intangible assets, match-making and visibility-enhancement, and various other activities can be eligible for state support under the condition of the GBER. Based on the GBER schemes, direct or indirect aid in support of cyber/defence ecosystem activities can be eligible, however a separate assessment will be necessary for each activity, and in designing the precise conditions and requirements for support/aid.

6.4.2. Intellectual property rights (IPR)

The source task description made specific inquiry about intellectual property frameworks in the context of the cyber/defence startup ecosystem. The intellectual property legal frameworks are relevant in a startup ecosystem for all stakeholders, yet the focus may vary.

A key element in determining the value of a startup (including in the initial phase of the project, before formal establishment of a vehicle/company) is the existing intellectual property and also future intellectual property that will be created. At the ideation stage, founders create codes, designs and other intangible assets, which, in the absence of a contrary contractual arrangement or employment relationship, comprise the intellectual property belonging to their creators/authors. It is of utmost importance to clarify what intellectual property exists related to a startup, who owns it and to make sure - if needed - that the intellectual property rights (IPR) belong to the startup, more precisely to the legal entity that will be the recipient of various support measures and investment. This is typically a contractual question, relatively easily addressed in IP assignment and licence agreements between the founders, key personnel (creators/authors and owners of the IPR) and the startup company, as appropriate.

Oftentimes, startup teams ask friends, classmates, family members or just random people solicited online to contribute with some idea, logo or sketch or piece of code, etc. The same practical solution of IP assignment and licence agreements is recommended in these cases also, however, where there is reluctance to sign over the IPR or impossible to track down the actual creator/owner, it may be suggested that the IP is not used, or the situation is highlighted as a significant risk.

One challenging area here may be the ownership of IPR when cyber conscripts create IP as part of their tasks during the service time. In particular copyright, especially relevant for copyright in software, in works created under employment contract or in public service is transferred to the employer unless otherwise prescribed by contract.[74] This may create the less than ideal situation that if there is interest in using the IP for developing a commercially viable product and for the startup it would be necessary to own the IP, it may be practically difficult to sort out and achieve an effective assignment of IP from employer/state to the startup/founder. It would require further in depth analysis to assess the merits of keeping

[74] Art. 32(1) of Estonian Copyright Act.

state ownership in IP created by conscripts. However, from the perspective that the aim is to develop competitive products, there is a strong argument that conscripts could keep ownership of IP they create, or under certain circumstances (such as end of service period and participation by the conscript in the cyber ecosystem programme), the IP could be transferred back automatically. With this system, the actually used IP can be managed efficiently by private sector (without the red tape in public sector). It was pointed out that conscripts leave before products could fully be developed, thus it is presumed that there is some IP created during their service, which is left unused. For these cases, it may be considered to keep state ownership of the IP, create a repository and licence the eligible IP to interested parties for free/under an open source regime. This solution would raise the chances that good ideas are not wasted and somebody could pick up on them and continue. It is recommended to clarify the ownership and assignment of IPR with conscripts during their service time, and create a system which would allow conscripts to take IPR "with them" under certain circumstances. This can be achieved by contractual arrangements.

Singapore's national IP protocol may be a source of inspiration for designing the mechanisms and content for such contractual arrangements (see in 3.4.). As a general principle Singapore public agencies should, in general, reserve a royalty-free, irrevocable, worldwide, perpetual and non-exclusive right to use any licensed or assigned IP for their statutory functions, non-commercial and/or R&D purposes. Singapore public agencies should consider the commercial interest of the third party before applying this principle and act in a manner that supports the effective commercialisation of the IP by the third party. A similar approach may be adopted for the purposes of the Estonian cyber/defence ecosystem, however the retention of some IPR by the state/public agencies would require a case-by-case analysis and should be applied in a flexible manner keeping in mind that IPR are key assets for startups and such state/public agency rights may be seen by potential investors as lowering their value.

The importance of IPR assignment and licence provisions are emphasised in many processes and stages of startup support, which reduces the risk of mishandling IP. Relevant rules are included in the term sheets, shareholders agreements, management agreements, employment agreements, service agreements with IPR assignment, trainings, advisories and as a good practice templates are created to address typical situations, eg. founder transferring IPR to startup. The IPR management is a key element in the operation of a startup ecosystem and needs dedicated resources and strategy.

Perhaps most often relied on IPR frameworks are copyright and trade secrets regarding the ICT-related startups, since these involve software codes, in which cases copyright protection automatically arises if the code is original and fixed in a tangible medium. Business secrets, for instance closed source proprietary software assets can most practically be protected by trade secret practices and frameworks (more simply put: by keeping confidentiality, which can be addressed in confidentiality and non-disclosure agreements). Furthermore, one can also mention the relevance of trademark frameworks that can protect logos, trade names, etc. and relatively early on in the startups lifetime can come into focus (eg. trademark registration). Patent frameworks, however are less often used, one interviewed startup mentioned that patent application was filed as a sort of 'insurance', but in reality the protection is

underexploited since enforcement requires disproportionally large effort, energy, time and resources.

One should also point out that the IPR frameworks that potentially apply in an outward-looking and open startup ecosystem are often beyond the national boundaries. Furthermore, the EU IPR frameworks have laid down the common rules for the most parts and relatively little is left for national discretion. The copyright rules in Estonia derive from the Copyright Directive Directive (EU) 2019/790, the Software Copyright Directive (EU) 2019/790 and case law, such as Nintendo case CJEU C-355/12, Usedsoft vs Oracle CJEU C-128/11, SAS vs WPL CJEU C-406/10, and others. Trademark frameworks derive from the (Directive (EU) 2015/2436) (the Trade Marks Directive), and the EU Trade Mark Regulation (Regulation (EU) 2017/1001) addresses EU trade marks. Trade secret legislation is harmonised across the EU by the Directive (EU) 2016/943. For export-oriented businesses, the national patent framework is unlikely to be attractive, and thus EU patents and other jurisdictions are most relevant.

However, patents require a closer look, especially in the context of this report. First, it should be noted that eligibility criteria for patent protection differ among jurisdictions, and particular concern is about software patents in the EU and the US. Since the technical description of this project tasks was particularly concerned with the cybersecurity context, two scenarios should be distinguished. A) Invention/solution is created which is entirely software based, B) Invention/solution is created which is partially or fully hardware based.

Article 52 of the European Patent Convention excludes from patentability programs for computers as such. However, based on case law (starting with Vicom case in 1986[75]), computer-implemented inventions that provide a technical solution to a technical problem, so bring about a technical effect, can still be eligib/le for patent protection. Therefore, in the cyber-realm only solutions/software that bring about a further technical effect that goes beyond the normal physical interaction between the program and the computer, and also fulfil the rest of the criteria (are new, involve an inventive step and are susceptible to industrial application), may be eligible for European patent.

However, the US patent framework is more permissive and it is known about granting patents to software, business processes, methods, etc.

Furthermore, and put it into the context of long sales cycles of cyber/defence startups, high costs of patent applications, disclosure requirements of the subject-matter, targeted market and/or exclusion of the jurisdictions of competitors, each case requires an in-depth IPR strategy. At the level of the ecosystem, it would be a key function to support startups in devising their IPR strategies, but also enable them to implement potentially proactive IPR strategies (i.e. identifying and taking action to terminate infringements), which require significant resources. Availability of IPR resources and capabilities would also serve the purposes of startups that may opt for a more defensive IPR posture, since they may be targeted by patent and other IPR litigation (see for example patent trolls that strategically target startups). In addition, the differences in patent frameworks may lead to innocent

[75] T 0208/84

infringements of patents, that is a startup unknowingly applying a method that enjoys patent protection in the jurisdiction of the target market.

6.4.3. Other legal aspects

It is briefly mentioned here that depending on the exact context, deployment environment and functions of a solution provided by a startup within the ecosystem, various legal regimes may be applicable. Staying with the example of cybersecurity startups, they may have to prove compatibility with relevant standards, such as ISO/IEC 27001 or the Estonian Information Security Standard. This is also relevant if the startup is operating within or provides a service for an essential service operator within the meaning of the NIS Directive[76] (as implemented by Estonia's Cybersecurity Act[77]). NB! The NIS2 Directive[78] is expected to be soon adopted and will broaden the scope of subjects required to implement state of the art security measures. Furthermore, there are several other areas and sectors, where specific security standards have been established.

Last, but not least, and again depending on the functions of the solution provided by the startup in the ecosystem, certain legal obligations may arise from international laws, such as Hague Conventions, Geneva Conventions, principles and customary international law. One of such scenarios is in the case of cyber offensive tools, where potentially a weapons review should be conducted. Overall, the legal considerations greatly depend on the profile of the startup, and in this very swiftly developing legal environment there is a risk that the regulatory burden of cybersecurity startups will increase.

ANNEX 1 - INTERVIEW QUESTIONNAIRE

Qualification questions

Where are they incorporated?

Which year?

Name of the startup/Person - Blind if requested

Scope of questions

Describe their startup/other journey till now?

From the government perspective what ministries, govt proxies etc build up the ecosystem?

What things from this specific ecosystem did they interact with?

[76] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[77] Küberturvalisuse Seadus.

[78] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985

What things were available to them but they did not interact with?
What ecosystem features were missing to them?
Are there any ecosystem services that they used from other ecosystems?
What would have they liked to have in their own host ecosystem?
What impact would this have on their trajectory?
How did they handle IP in their host ecosystem?
Did any elements of the ecosystem hamper or assist them with IP?
Do they have any patents? If so where? If not why not?
How do funding sources get vetted? Screening of investments? LPs or sponsporship?
What constructions are used to provide financial or other support? Is there a government funding opportunity? Proxy?
Are there any export control regimes in place and how does that affect the startups markets?