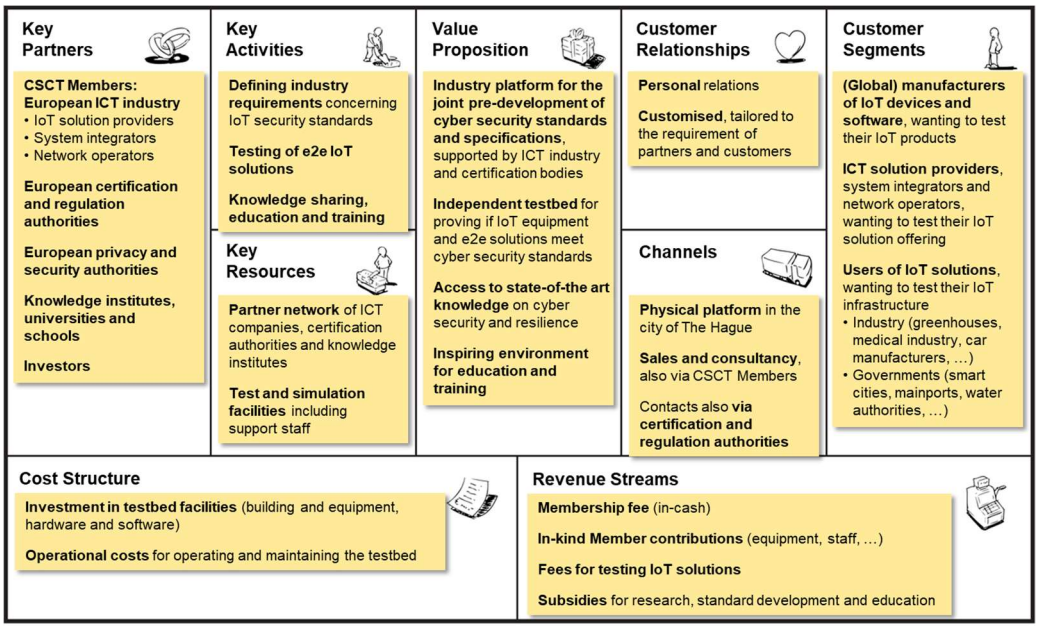
Towards a 'Cross Sector Cyber Testbed' in the MRDH-region[1]

Building a secure and resilient digital future together

Cyber security and resilience become increasingly important
In modern society, ICT is becoming ever more important. Numerous innovations are driven by developments in hard- and software and the application thereof. At large scale, new and promising Internet of Things (IoT)-applications are being implemented by companies, governments and civilians. This changes the way in which we work, communicate, travel, etc. The impact on society is huge. As a result, cyber security and resilience become more and more important, which is also emphasised in the Dutch government coalition agreement that was published in October 2017.

Testbeds are deemed indispensable for improving cyber security and resilience
A cyber testbed is "a platform where operators and manufacturers can test their hardware and software in a protected simulation environment".[2] As a recent feasibility study proved, setting up such a testbed in the MRDH-region could contribute considerably to raising the level of cyber security and resilience. The study pointed out that "there is an opportunity for a new platform, in which knowledge institutes, critical infrastructure managers, ICT companies and start-ups cooperate to accelerate innovation with respect to new cyber security technologies and methods and via which societal risks are minimised and mitigated by means of self-regulation and continuous testing of requirements." [3] According to the study, the IoT represents a new and very promising field of play for such a testbed.

The 'Cross Sector Cyber Testbed' (CSCT) as an industry pre-standardisation platform on IoT
In answering the need for increased safety, ongoing standardization and certification of IoT are crucial. As a pre-standardisation platform, the envisioned CSCT aims to fulfil a pivotal role in enhancing society's digital safety. In the CSCT, European industry and certification authorities will work closely together in defining the requirements for industrial IoT cyber security standards, as input for standardisation and certification. With its advanced and unique testbed facilities, the CSCT will also test IoT equipment and end-to-end solutions according to these standards, for industry and their customers. As such, the CSCT is unique and differs significantly from other, existing testbeds. Its business model is illustrated below.



[1] The Rotterdam The Hague Metropolitan Area (MRDH).
[2] 'Securing Critical Infrastructures in the Netherlands, towards a National Testbed', published by the HSD in 2015.
[3] 'Verkenning van Nut, Noodzaak en Haalbaarheid van een Nationaal Cybertestbed', TNO, HSD en MRDH, 2016.

The CSCT value propositions address a clear need from industry. As a recent benchmark among 400 technology leading companies shows, “cybersecurity issues remain top-of-mind for executives”.[4] According to the study, 32% of the respondents mentioned security and privacy risks as a barrier to their organisation’s efforts with respect to data-related initiatives. The CSCT aims to lower this barrier and aims to become a world leader in setting the requirements for industry IoT security standards and for testing real-life IoT-based systems and solutions.

Industry, government and knowledge institutes support setting up the CSCT
Different parties have expressed their commitment to support the establishment of the CSCT. Among these are the Ministry of Security and Justice, The Ministry of Economic Affairs, The Ministry of Defence, the City of The Hague, the City of Rotterdam as well as the Hague Security Delta (HSD). Moreover, KPN, Cisco, Siemens, Thales, the Port of Rotterdam, Greenport and several large banks and have expressed their interest. The Dutch Institute for Applied Scientific Research (TNO) has taken the lead in preparing a business plan for the CSCT. The first use case with the Dutch regional water authorities to test the end-to-end security of the LoRaWAN sensor network already started (involving among others KPN and TNO), to give the CSCT a flying start.

The CSCT will actively pursue international cooperation
To be able to grab the chances digitalisation offers, cyber security must be in order. The only way to succeed for companies, knowledge institutes and governments is to join forces - both nationally as internationally. Therefore, the CSCT is foreseen to closely cooperate with other national and international organisations focussing on improving cyber security. Links with for example the Singapore University on Technology and Design (SUTD), the Control System Security Centre (CSSC) in Japan and CyberNB in Canada have already been established.

Location of the CSCT will be the city of The Hague
“Over the year 2014 and 2015, the city of The Hague has become a Cybersecurity Gateway in Europe, now hosting the NCIA, Eurojust and the EC3. As such, The Hague is turning into the cybersecurity capital of Europe.” [5] Numerous cyber and ICT firms and start-ups are based in The Hague, like the cyber security department of TNO. The city of The Hague also hosts the HSD, the largest security cluster in Europe. From this perspective, a choice for The Hague is logical.

Moreover, The Hague was selected by the Rockefeller Foundation as one of the one hundred Resilient Cities: “Known as the international city of peace and justice, The Hague has built a strong reputation as the home to key international organisations, including the International Criminal Court. The city’s long-term resilience depends on cybersecurity, and The Hague has explicitly focused on security innovations and the development of resilience in the face of cyber-attacks. However, continuous technological development requires the city and its partners to continue to strengthen security and monitor for vulnerabilities in its digital infrastructure.” [6]

The CSCT is an integral part of the regional strategy of the MRDH
The Roadmap Next Economy (RNE) of the MRDH identifies five transition paths. Smart Digital Delta is one of these. According to the RNE, Smart Digital Delta is about “Everything that the region needs to increase data productivity and take the step towards a digital economy: better digital connections, networks, platforms and big data.” One of the facilitating projects to enable the development into a Smart Digital Delta comprises the establishment of a CSCT. The CSCT will contribute to realising the region’s ambition, will stimulate innovation in ICT and will further foster employment in the region.[7] This will be elaborated in a business plan for the European investment Bank, that will be prepared over the coming months.

[4] ‘From Cloud, Mobile, Social, IoT and Analytics to Digitization and Cybersecurity’, Protiviti, 2016.
[5] ‘Securing Critical Infrastructures in the Netherlands, towards a National Testbed’, published by the HSD in 2015.
[6] http://www.100resilientcities.org
[7] In 2015, the region already showed a 12 percent increase in jobs in the field of cyber security, proving this sector’s viability.