Background per Country

United States of America

President Obama has identified cybersecurity as one of the most serious economic and national security challenges for the United States, but one that the U.S. as a government or as a country is not adequately prepared to counter. The U.S. is therefore actively supporting and engaging industry, academia and other nations to help build the necessary cyber capabilities and workforce. Capabilities that effectively counter emerging new threats in cyber space and ensure that the digital infrastructure is secure and trusted to enable further international trade and economic growth.

The global market for cyber security products and services is rapidly growing. Yet the U.S. offers a especially lucrative market since the annual cyber security spending of the US Federal government alone is bigger than any national cyber security market including both public and private sector. With a cumulative market valued at $65.5 billion (2015–2020) and growth of around 6% per year, the U.S. federal cyber security market exceeds at least twofold the largest cyber security spending countries.

Major investments in the U.S. cyber security space range from federal spending on R&D for the protection of critical infrastructures (e.g. DHS, DOE), public-private partnerships on information sharing and maturity models (e.g. NIST) to record level of venture funding in start-ups ($1.71 billion in 2013). These activities tend to concentrate in certain hot spots in the U.S. including the Washington DC Metropolitan are incl. Virginia and Maryland, San Diego (CA) and San Antonio (TX). Furthermore, as a policy the U.S. is investing in cyber space diplomacy through international partnerships and coalition to combat cybercrime and foster an open, free and secure internet.

All this provides a unique opportunity for Dutch entrepreneurs, researchers and policy makers to work with the U.S. and actively pursue relationships for business development, research and innovation as well as policy. The Netherlands embassy has supported and invested in these relationships over the past years which has resulted in economic missions and matchmaking events generating many new business opportunities, in MOU's with several U.S. hot spots to open up new networks and exchanges, collaborative R&D projects as part of a new S&T treaty between the U.S. and the Netherlands as well as improved government relations. The challenge will be to further invest in and build upon these activities and commitments and position the Netherlands as the main European trade, investment and innovation partner for the U.S. in cyber security.

Japan

A series of remarkable cyberattacks on government and private targets (including Sony, Mitsubishi, Yahoo Japan, National Pension Administration) have firmly placed cybersecurity on the political agenda in Japan. In 2020 the city of Tokyo will host the Olympic and Paralympic games. This spells opportunities to show-off Japan's economic and technological prowess, but it also poses challenges in cyberspace. How to protect the megapolis' critical infrastructure for the 40 million inhabitants and participants will be a top-priority (electricity, communication, water and sewage, railways). The training of plentiful, capable staff and exercises for incident response has been stated as a key priority for the Japanese government, which is coordinating efforts through its National center of Incident readiness and Strategy for Cybersecurity (NISC). The current size of the market for cybersecurity products and services is estimated at around 6 billion euro, with a 3% predicted annual growth rate.

Over the past two years, the Netherlands Embassy in Tokyo and RVO have organised 5 consecutive cybersecurity missions to Japan. They have been an example of public-private-academic collaboration, with participants from all fields jointly opening doors for each other. There have already been concrete results. Research partnerships have been established between The Hague-based European Network for Cyber Security (ENCS) and several Japanese cybersecurity research institutes. Commercial contacts were established for several small, medium and larger enterprises with key Japanese players. The partnership between RedSocks (NL) and Networld (Japan) is perhaps the prime example. Overall, the Netherlands government has shown strong support for bilateral collaboration with Japan in the field of cybersecurity. Prime Minister Rutte and Minister for Economic Affairs Kamp supported the Dutch cybersecurity sector during their recent visit in November 2015. The state visit of His Majesty King Willem-Alexander and Queen Máxima was accompanied by an economic mission in October 2014, including a cybersecurity delegation. Minister Kamp joined this mission during the Japan-Netherlands Cybersecurity Roundtable.

Netherlands Enterprise Agency

Singapore

Cyber security and innovative financial technology solutions are high priority in Singapore.

A few years ago, the Singapore government has launched a five year National Masterplan 2018 on Cyber Security Singapore with the objective to stimulate development of capabilities in the aforementioned areas and to create a cyber-security hub for the region. In the same context, Singapore has taken the lead role in the Association of South East Asian Nations (ASEAN) to generate cyber security policies and to provide a know-how and talent pool for the region. In order to achieve these objectives, the government has reserved substantial amounts of Singapore dollars, that will be made available through annual grant calls by the National Research Foundation (NRF). Finally, the Singapore government has created the so-called cyber security agency. The CSA is the national body to coordinate the cyber security strategy, education and outreach and industrial development.

To Singapore, international cooperation is a key success factor, in order to have access to highly qualified personnel, industrial solution providers with state-of-the-art products and services and to stay ahead of the cyber threats.