On 19 May the Dutch National Science Foundation (NWO), the Ministry of Security and Justice (V&J) and the US Department of Homeland Security (DHS) signed an agreement for a joint cyber security research project with title: 'Increasing the impact of voluntary action against cybercrime'. Based on this agreement Dutch scientist Michel van Eeten (TU Delft) and his American colleague Tyler Moore (Southern Methodist University) have started their joint research aiming at an evidence-based design for fighting cybercrime. *Door Bennie Mols*

'Technology alone is not going to fix cyber security problems'

Michel van Eeten and Tyler Moore just before the kick off of their joint research project 'Increasing the impact of voluntary action against cybercrime' at the NCSRA Symposium in The Hague

What is the main aim of your joint research project?

Tyler Moore: 'Most of what is being done today to protect people against cybercrime is carried out by private actors and not by law enforcement. Yet, even if people are not required to act, they do. We are looking at the underlying organizational infrastructure, rather than at technology of an attack. We want to understand better how voluntary actions against cybercrime works. How effective are they at present? How can they be made more effective?'

Can you give a concrete example?

Michel van Eeten: 'Let's assume you find a phishing site. You report the site to the anti-phishing site PhishTank. PhishTank then has a variety of mechanisms to further disseminate the information of where these phishing sites are hosted. Typically it is hosted on a legitimate domain that got hacked.'

Tyler Moore: 'It is often difficult to identify who is the owner of the phishing site, so you may need the hosting provider to take action. But sites do get disinfected every day. We want to look at how effectively this is done.'

Agreements associated with these projects were recently signed in Washington, D.C. by Pieter Cloo, Secretary General of the Ministry of Security and Justice, Reginald Brothers, Under Secretary for DHS S&T and Louis Vertegaal Director NWO-CEW.
Greg Wigton, Luke Berndt, Ann Cox, Reginald Brothers, Douglas Maughan,Eelco Stofbergen, Pieter Cloo, and Jan Piet Barthel

On 2 June two of the three DHS-NWO cyber security research projects were kicked off by their Principal Investigators during the NCSRA Symposium in The Hague (about the execution of the Dutch National Cyber Security Research Agenda). The kickoff of the third joint research project will take place in Washington, D.C. in August this year.
Alfonso Valdes, Tyler Moore, Sandro Etalle, Michel van Eeten, Douglas Maughan and Louis Vertegaal

American-Dutch cooperation in cyber security

The Dutch National Science Foundation (NWO) and the US Department of Homeland Security (DHS) Science and Technology Directorate cooperate on three projects in the field of cyber security research. These projects fit under the Dutch American Project Arrangement about cooperative research and development on cyber security, ratified by the Ministry of Security and Justice and DHS:

1 *Malware on smartphones: collection, analysis, and defensive measures*
Herbert Bos (VU University Amsterdam, NL)
Christopher Kruegel (University of California Santa Barbara, US)
2 *Increasing the impact of voluntary action against cybercrime*
Michel van Eeten (Delft University of Technology, NL)
Tyler Moore (Southern Methodist University, US)
3 *In-depth defense of SCADA and industrial control systems*
Sandro Etalle (University of Twente, NL)
Alfonso Valdes (University of Illinois at Urbana Champaign, US)

Michel van Eeten: 'Every day thousands or maybe even tens of thousands of phishing sites are taken down. We want to generalize from the concrete examples that we will study. When criminal cyber activity is detected, abuse reports are being sent to certain parties, asking them to act. The big question is how to make these more effective. How much information is optimal? Is it better to send a full technical description of the attack? Or is it better to send only a very simple message?'

Tyler Moore: 'By studying this problem, we want to take lessons from behavioral economics. We need to know the incentives from the side of the defender. Technology alone is not going to fix security problems. You need a combination of technology and human factors to make progress. Therefore our research is a blend of computer science and social science.'

Does the project have clear deliverables?

Tyler Moore: 'We have broken up our project in three concrete parts. The first part consists of building a taxonomy of notification regimes: which notifications are being sent during which attacks? You can see this as mapping of what is already being done to fight cybercrime. The second part consists of observational studies in which we are going to measure the effectivity of all kinds of abuse reports. The third and last part consists of running what we call 'quasi-experiments'. We want to try experimentally in the real world which notifications do work and which ones don't work.'

The internet will be expanding to all places and all devices. How optimistic or pessimistic are you about the future of fighting cybercrime?

Michel van Eeten: 'Looking at the past, I can only say that all the doomsday scenarios have failed. So, I do not believe that cybercrime is only getting worse in the future. I would say that we are getting to a continuous push and pull between cyber attackers and cyber defenders. You can see it as a dynamic equilibrium, exactly in the same way as with shop theft or robberies in the physical world. Sometimes the thieves are a bit ahead, sometimes the police is a bit ahead.'

Tyler Moore: 'Looking at worst case scenarios does not help. What we need is better measurements of both cybercrime and cyber defense. And I do hope that our project will lead in three or four years to evidence based recommendations that will be adapted by the cyber security industry.' I/O

More information
www.nwo.nl/cybersecurity