Long Term Cybersecurity research
Summaries of projects granted in the second NWO call for proposals (2014)

Project number	CYBSEC.14.003 / 628.001.016	
Main Applicant	Prof. dr. ir. C.T.A.M. de Laat	Universiteit van Amsterdam Faculteit der Natuurwetenschappen, Wiskunde en Informatica Instituut voor Informatica
Project title	Security Autonomous Response in programmable Networks (SARNET)	

Scientific summary

The ever wider use of ICT in our society is reflected in the growing complexity of ICT systems and probably, the growing number of cyber criminals. These growing numbers impact the risk of cyber criminality adversely. Risk is an important concept in our research, it is the average impact of a given malicious interaction with an ICT infrastructure. As one of the partners of this proposal, Air France-KLM, has experienced these impacts, which can be enormous.

Basically our research goal is to obtain the knowledge to create ICT systems that model their state (situation), discover by observations and reasoning if and how an attack is developing and calculate the associated risks. In addition, our goal is to have the knowledge to calculate the effect of counter measures on states and their risks, and to choose and execute one. In short, a we research the concept of a networked computer infrastructures exhibiting SAR: Security Autonomous Response.

Based on prior research, we are capable to use the new technologies of Software Defined Networking (SDN), cloud computing and Network Function Virtualisation (NFV) for SAR, e.g. to adapt a network topology as a response to a threat. In earlier research we learned how to create software (control programs) that continuously control ICT infrastructures.

Multi country test beds, visualisation centres, public workshops and whitepapers are part of our validation and valorisation activities. The research is supported by Ciena, a network equipment manufacturer and will be validated in the context of Air France-KLM.

Applicable NCSRA themes

- Attack detection, attack prevention and monitoring
- Data, Policy and Access Management
- Secure Design and Engineering