SARNET
Secure Autonomous Response Networks
Ralph Koning (UvA), Ameneh Deljoo (UvA), Robert Meijer (TNO), Leon Gommans (KLM), Tom van Engers (UvA), Rodney Wilson (Ciena), Cees de Laat (UvA)

SARNET
SARNET, Secure Autonomous Response NETworks, is a project funded by the Dutch Research Foundation. The University of Amsterdam, TNO, KLM, and Ciena conduct research on automated methods against attacks on computer network infrastructure. The research goal of SARNET is to obtain the knowledge to create ICT systems that
• model the system’s state based on the emerging behaviour of its components,
• discover by observations and reasoning if and how an attack is developing and calculate the associated risks,
• have the knowledge to calculate the effect of countermeasures on states and their risks, and
• choose and execute the most effective countermeasure.

Control loops
The SARNET framework uses control loops to maintain the security state of the network. Its similar to the OODA (observe, orient, decide, act) loop but adds more granularity and an extra learning step.
A SARNET has one or more security observables derived from the network’s policies. These observables are constantly monitored. When an anomaly takes place this triggers the control loop.

Software defined networking
By using the latest techniques in Software Defined Networking and Network Function Virtualisation, a SARNET can use advanced methods to defend against cyber attacks and return the network to its normal state.

SARNET Alliance
The subject of the SARNET alliance research is the value of collaboration between alliance members in terms of risk reduction, cost benefit and revenue impact.
The aim is to provide a-priori insight into the rationale of collaboration. Based on the Service Provider Group framework, the SARNET alliance institutionalises trust by arranging common rules, its execution and judgment. The research builds distributed computational models of an alliance that analyses the policies each autonomous member constructs from the common set of rules.
The models can become part of an Information Security Management System that establishes, reviews, maintains, and improves information security amongst alliance members.