Trasporti, industrie e per la prima volta anche droni. Erano questi gli ingredienti principali di "Locked Shield 2016", la più grande simulazione di cyber-defense al mondo che si è appena conclusa al Cooperative Cyber Defense Centre of Excellence della NATO a Tallin, in Estonia. Quest'anno hanno partecipato 19 nazioni e per l'Italia, accanto ai militari del Comando C4 dello Stato Maggiore della Difesa, anche due giovani esperti del dipartimento di Informatica dell'Università di Pisa.

Per due settimane Federico Tonelli, che sta svolgendo il dottorato, e il suo collega Lorenzo Isoni, borsista, hanno partecipato all'esercitazione e difeso l'immaginaria nazione di Berylia da un violento attacco informatico degli hacker del team NATO.

"Al centro dell'esercitazione – ha spiegato il professore Fabrizio Baiardi dell'Ateneo pisano che ha coordinato a distanza le operazioni – c'era la protezione del sistema dei trasporti e degli impianti industriali e ogni squadra aveva inoltre un drone da difendere da collisioni e incidenti. Per rendere l'idea di cosa significhi un attacco informatico in questi ambiti basta immaginare ad esempio una smart city dove una banda di criminali manipoli tutti sistemi di controllo dei semafori o un terrorista che prenda il controllo di una centrale per la produzione di energia o una rete per la distribuzione del gas ".

E' il terzo anno che gli esperti dell'Università di Pisa sono invitati a partecipare a Locked Shield. Dalla prima edizione nel 2010 l'esercitazione è divenuta sempre più articolata e complessa e in totale quest'anno ha coinvolto oltre 550 specialisti di diverse nazioni impegnati nella protezione di complesse infrastrutture informatiche realizzate ad hoc.

"Dal punto di vista tecnico il nostro ruolo – ha concluso Fabrizio Baiardi - è stato di applicare gli strumenti dell'ambiente Haruspex per analizzare la rete informatica che era il 'campo di battaglia' di Berylia e di fornire alla squadra del nostro paese le modifiche necessarie per renderla il più resistente possibile agli attacchi degli hacker NATO".

Sviluppato in un progetto pluriennale coordinato dal professor Fabrizio Baiardi e dall'ingegner Marcello Montecucco della Fondazione Promostudi di La Spezia, Haruspex è infatti un insieme integrato di strumenti software in grado di individuare ed eliminare i punti deboli delle reti informatiche in modo automatico. Alcuni strumenti analizzano la rete ICT per individuarne i difetti, altri prevedono come la rete sarà attaccata e suggeriscono le modifiche da realizzare per renderla sicura.