Europe's cybersecurity policy settings under attack

May 4 2014, by James Panichi

Even as Europe powered up its most ambitious ever cybersecurity exercise this month, doubts were being raised over whether the continent's patchwork of online police was right for the job

Even as Europe powered up its most ambitious ever cybersecurity exercise this month, doubts were being raised over whether the continent's patchwork of online police was right for the job.

The exercise, called Cyber Europe 2014, is the largest and most complex

ever enacted, involving 200 organisations and 400 cybersecurity professionals from both the European Union and beyond.

Yet some critics argued that herding together normally secretive national security agencies and demanding that they spend the rest of 2014 sharing information amounted to wishful thinking.

Others questioned whether the law enforcement agencies taking part in the drill should be involved in safeguarding online security, in the wake of American whistleblower Edward Snowden's revelations of online spying by western governments.

"The main concern is national governments' reluctance to cooperate," said Professor Bart Preneel, an information security expert from the Catholic University of Leuven, in Belgium.

"You can carry out all of the exercises you want, but cybersecurity really comes down to your ability to monitor, and for that, national agencies need to speak to each other all the time," Preneel said.

The Crete-based office coordinating the EU's cybersecurity, the European Union Agency for Network and Information Security (ENISA), calls itself a "body of expertise" and cannot force national agencies to share information.

As with most aspects of policing and national security, the EU's 28 members have traditionally been reluctant to hand over powers to a central organisation, even when—as in the case of online attacks—national borders are almost irrelevant.

'Citizens and economy at risk'

Cyberattacks occur when the computer information systems of

individuals, organisations or infrastructure are targeted, whether by criminals, terrorists or even states with an interest in disrupting computer networks.

The EU estimates that over recent years there has been an increase in the frequency and magnitude of cybercrime and that the attacks go beyond national borders, while the smaller-scale spreading of software viruses is also an increasingly complex problem.

The EU's vulnerability has been highlighted over recent years by a number of high-profile cyberattacks, including one against Finland's foreign ministry in 2013 and a network disruption of the European Parliament and the European Commission in 2011.

And with Europe's supply of gas from Russia focusing attention on energy security, the highly computerised "smart" energy grids which transport and manage energy in the EU are also seen as vulnerable.

Yet the view from Brussels is that the member states' reluctance to work together on cybersecurity amounts to "recklessness", with one EU source saying national governments were "happy to put their citizens and economy at risk rather than coordinate across the EU."

ENISA was established in 2001 when it became clear that cybersecurity in the EU would require a level of coordination. Unlike other EU agencies, ENISA does not have regulatory powers and relies on the goodwill of the national agencies it works with.

The agency is undaunted by its task, arguing that the simulations it stages every two years, taking in up to 29 European countries, are both effective and necessary in preparing a response to cyber-attacks.

This week's simulation created what ENISA described as "very realistic"

incidents in which key infrastructure and national interests came under attack, "mimicking unrest and political crisis" and "disrupting services for millions of citizens across Europe."

Responsibility with industry

However, Amelia Andersdotter, a Swedish member of the European Parliament with the libertarian Pirate Party, is dismissive of both the exercise and the European online security model.

Andersdotter, along with a number of European experts, is calling for reforms to move responsibility for cybersecurity away from law enforcement agencies toward civilian bodies.

Their argument is that a civilian agency would be better placed to coordinate a response with industry, which Andersdotter argues has not done enough to safeguard cybersecurity.

At present, she told AFP, industry actors in software or infrastructure simply report cybercrime to authorities without being required to compensate or inform consumers.

A civilian authority would end what Andersdotter calls the "conspiracy of database manufacturers and law enforcement agencies" by placing greater responsibility with industry.

What most experts agree on is that European companies and consumers are vulnerable to cybersecurity threats, and that can have an impact on people's willingness to use online services.

James Wootton, from British online security firm IRM, said the ENISA exercises are a step in the right direction, but are not enough.

"The problem is nation states wanting to fight cybercrime individually, even when cybercrime does not attack at that level," Wootton says, arguing that national law enforcement agencies often lack the required resources.

"So it is good to look at this at the European level, but what power does ENISA have? What can they force countries to do?"

Eurostat figures show that, by January 2012, only 26 percent of EU enterprises had a formally defined information technology security plan in place.

One industry insider said the view in Brussels is that EU cybersecurity was "like teenage sex: everyone says they are doing it but not that many actually are."