Are the Real Limits to Scale a Matter of Science, or Engineering, or of Something Else?

Ross Anderson
University of Cambridge
Cambridge, England

Abstract—As people get excited about the latest idea for "Big Data" and the "Internet of Things", computer people often shake our heads and say "It won't scale." Pessimism isn't always justified: we have been able to scale up quite a number of tasks, from connectivity through search to social media. But other applications are recalcitrant, from energy management to medical records. The conventional computer-science view is that scaling systems is about computational complexity; about whether the storage or communications required for a task grows more than linearly in the number of users. Over the past thirty years we've developed a pretty good theory of that, but we're learning that it's nowhere near enough.

In this talk I present a complementary view, based on over thirty years' experience of security engineering, that the real limits to scale are usually elsewhere. Even where the data are manageable and the algorithms straightforward, things can fail because of the scaling properties of the social context, the economic model or the regulatory environment. This makes some automation projects much harder than they seem. When it comes to safety and privacy many of the attacks that are easy to do in the lab are rare in the wild, as they don't scale either. But others surprise us; no-one in the intelligence community anticipated a leak on the Snowden scale. In short, scaling is now a problem not of computer science but of systems engineering, economics, governance and much else. Conceiving problems too narrowly makes failure likely, while good engineering will require ever more awareness of context. The implications for research, education and policy bear some thought.)