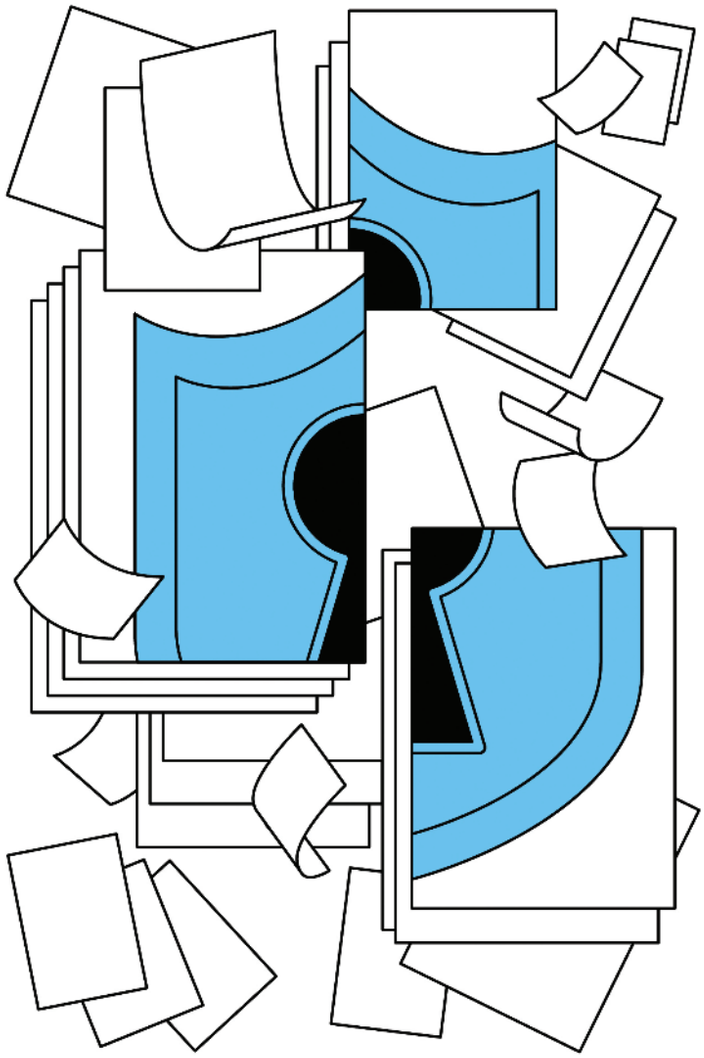

SNAPSHOTS

Uncovering the complex dynamics shaping EU cybersecurity policy

The exponential rise of digital products in the "Internet of Things" (IoT) age offers us all convenience and efficiencies—but also makes us more vulnerable to cybersecurity attacks. IoT devices often have weak security, which means our smart thermostats, fridges and fitness trackers can be hacked by bad actors who want to steal or manipulate sensitive data.

The European Union's efforts to address this issue have resulted in policies that may backfire on consumers, says Ido Sivan-Sevilla, a social scientist and technologist who is a professor at the University of Maryland's College of Information Studies. He unpacks this phenomenon in his study "Europeanisation on demand: the EU cybersecurity certification regime between market integration and core state powers (1997–2019)" (*Journal of Public Policy,* August 2020). Through interviews with 18 government and industry stakeholders and a review of 41 relevant policy documents, Sivan-Sevilla tracked two decades of policy development in EU digital security certification, concluding with the 2019 EU Cybersecurity Act.

Sivan-Sevilla found that inconsistent attempts to follow economic integration practices in cybersecurity have led to alarming gaps in policy development. Despite promises by EU policymakers to fundamentally change the existing non-functional, fragmented and nationally oriented certification ecosystem, the 2019 act created a regime that largely maintained the status quo.

As well, Sivan-Sevilla showed that it was in the best interests of almost all parties involved—the European Commission and its member states—to only slightly diverge from existing arrangements. In particular, powerful member states—France, Germany and the UK—wanted to maintain their political sovereignty over cybersecurity issues and opposed the commission's efforts to gain decision-making powers over the cybersecurity apparatus.

What has emerged is a model that Sivan-Sevilla calls "Europeanization on demand," wherein certification of digital products across the EU happens on a case-by-case basis. Authorities in member states still decide on the level and extent of integration based on national interests, he says, but supranational institutions such as private cybersecurity certification bodies may play a bigger role in certifying products on behalf of the EU.

"Because EU nations want to maintain decision-making powers, it leads to suboptimal cybersecurity policy outcomes," says Sivan-Sevilla, who previously was an Azrieli Graduate Studies Fellow at the Hebrew University of Jerusalem, a postdoctoral fellow at Cornell Tech and a Fulbright Scholar at the University of Minnesota. "As economic and sovereignty-related policy issues shape cybersecurity policy, we need to monitor how political compromises in this arena may affect the public interest." ■