Opinion | 5 December 2018

Julian King: Securing the Digital Revolution

The world is hurtling toward a more decentralized digital future, characterized by unprecedented linkages among people, data, and objects. In order to reap the benefits of innovation, without creating massive vulnerabilities, we need to anticipate and address the threats now, **writes Julian King**

Julian King, a former British ambassador to Ireland and France, is the EU Security Union Commissioner

Another connectivity revolution

Pity the person who invests heavily in canals right before the railways start operating. You could understand, for example, why the sponsor of the Bridgewater Canal (perhaps England's first) would vehemently oppose the planned Liverpool and Manchester Railway. But the march of technology could not be stopped – nor could the new challenges it raised.

The same is true of today's digital innovations. When the L&M Railway eventually opened in 1830, it was a revolutionary success, kickstarting the age of steam and changing the world in ways that could not have been foreseen. As the railway age unfolded, with metal tracks spreading across the industrializing world like veins on a leaf, a new level of connectivity was achieved, which criminals

were quick to exploit.

> *The word is on the brink of another revolution in connectivity*

Indeed, an entire police force eventually had to be created to manage railway security. With the world on the brink of another revolution in connectivity, especially in terms of infrastructure that will fundamentally change the way we connect with each other, the lessons of this experience should not be ignored. And the coming phase of the digital age will affect far more than just transportation. We are not talking about the Internet of Things, but about the Internet of Everything: a more decentralized digital future, connecting people, data, and objects like never before.

We must be alert to new security issues

In terms of security, we need to ensure we aren't sitting, as it were, on a slow-moving canal barge while the 8:15 to Manchester flashes past. We need to take a clear-eyed look at the strategic vulnerabilities that these technologies will bring, and anticipate how malicious actors could attempt to exploit new digital infrastructure for their own gain or to deploy it as a weapon.

Some challenges, such as the misuse of social media to spread disinformation – using, among others, cutting-edge tools like deepfake videos and artificial intelligence – are already clear.

But, crucially, we are also talking in terms of the infrastructure itself. The fifth generation of mobile communication technology, 5G, poses a particular challenge. It will be the backbone of global connectivity, which raises strategic and security questions about issues like supply-chain security and provenance. How can we be sure that the components used in future generations of European technology – not only 5G – will be secure?

Common standards and rules are required

Already, digital supply-chain security is far from airtight, reflected in recent reports of companies finding mysterious chips on their server motherboards, seemingly added at the time of manufacture. The British government has warned telecoms companies to consider their suppliers very carefully, while the United States has been looking to restrict some kinds of foreign direct investment in key technologies like semiconductors and robotics.

To secure the digital-infrastructure supply chain, we need greater transparency regarding the provenance of technological components. Maintaining a diversity of suppliers is also vital. Furthermore, common standards and rules are needed to establish the trustworthiness of international partners.

That is the basis of a recent proposal by French President Emmanuel Macron, described in the Paris Call for Trust and Security in Cyberspace. The Internet, according to Macron, has become a site of conflict, where malicious actors exploit the vulnerabilities of digital products and services. He proposes that Europe create an "Internet of Trust," based on lawfulness and cooperation. I agree. Europeans should be able to continue enjoying their online lives secure in the knowledge that their fundamental values and rights, such as free speech, are protected.

Future strategy

We need a strategy that balances our need to harness technological innovation in order to safeguard our economic future with the need to avoid creating massive security vulnerabilities in the process. And with the technology train already hurtling down the track, we must act fast to mitigate current risks and ensure that we are laying the groundwork needed to avoid future threats. In confronting this admittedly huge challenge, we need to avoid short-sighted responses, such as protectionism and other measures that stifle innovation. Instead, we must map the scale and extent of the risk, and decide what is truly strategic.

We need to avoid short-sighted responses

For Europe, this means not just protecting supply chains, but also pursuing large-scale, coordinated investment in our own tech industries. The European Commission is uniquely well placed to drive this cross-sectoral work. It is not too late for Europe to safeguard its digital future. Even the owner of the Bridgewater Canal eventually saw the way the wind was blowing – and invested heavily in the rival railway.

This article first appeared in Project Syndicate on November 26th, 2018