2019
HALIFAX
PAPERS

HALIFAX
INTERNATIONAL SECURITY FORUM

NOVEMBER 22-24, 2019

2020s VISION: RESPONSIBILITY TO PRO-TECH

— Pauline Neville-Jones

Big cyber incidents make the news. Stuxnet, Notpetya, Wannacry, and other such attacks designed to advance the political agenda of the originating country get headlines. But cyber enabled financial crime is now so ordinary that only the most egregious examples make the news. We live with heightened risk because we want the benefits of the digital world.

Control and use of data are the greatest sources of power and wealth creation in the 21st century. Attitudes to, and laws about, data are reshaping our societies and economies in fundamental ways, with profound differences emerging. The less the state has control over data and the less it is the source of innovation, the less powerful it becomes. The converse is also true.

In democracies, the position of the state has been diminished relative to both the individual and the private sector, which has become the primary source of innovation. "Big Tech"—which in the West means primarily American tech—has mushroomed into a powerful force based on profits made from the exploitation of data, not least personal data.

Through social media platforms, individuals and organizations have been able to communicate and organize politically without their authorship, or its location, being admitted or readily traceable. Distrust poisons the well. Government, in the name of the services it provides and its duty to protect the population from threats of military conflict, terrorism, extremism, violence, and organized crime, has to some extent pushed back on the limits placed on its access to personal data. But neither it nor other actors in society have yet found ways to ensure that free speech does not fall victim to false news and political division.

Contrast the redistribution of power across democratic societies with its concentration in states governed by authoritarian regimes, where control of all kinds of data is being accumulated by government, greatly increasing its power in relation to the citizen and the economy.

China is developing a social model which limits individual access to data, free speech, and association. Arguably, on the other hand, it provides the basis for unprecedentedly successful growth and technological progress, offering stiff competition to Western democracies, and attracting favorable attention in third countries. The assumption made in democracies that free enquiry is a necessary condition for economic and social success is not—yet at least—being borne out.

The two models will be tested over time for their resilience. Today, in China, Russia, and North Korea, the cyber world has become an agent of deniable action by the state or by criminals harbored within national borders, to sap the military, economic, and political strengths of their targets.

Denial and disruption of communications and infrastructure; extensive intellectual and financial property theft; and hybrid warfare-propaganda and information manipulation to the point of false news, are all tools of the trade in adversarial interstate relations.

In democracies, these externally generated threats result in economic loss, they help undermine

political and social consensus, and they assist the slide towards populism and political extremes. Innovation and competition unavoidably imply risk. The systemic fragility of the digital revolution brings with it significantly higher levels of technical risk than the preceding mechanical world, which adds to our challenges. Our failure to square up to risk management seriously means that sometime we will almost certainly experience disruption on a massive scale.

This shirking must change if we are to reduce the likelihood and impact of cyber attack. Producers should be liable for the quality of their software; users need to be better educated, and more diligent about managing risk; and the public and private sector together need to invest much more heavily in resilience—the ability to detect problems and recover from incidents quickly. These are essential conditions of the connected world of the Internet of Things.

Democracies must also find ways to reaffirm their political values in the face of the uses to which new technologies are being put. This is urgent for two reasons. First, the damage to the fabric of democracy is already visible. The private sector, especially social media companies, need to cooperate more closely with government in striking the balance between personal privacy and collective security. And in public life there needs to be a recognition that accountability, and not its evasion, is fundamental to the health of democracy.

The second reason is that the technological revolution has only just begun. We are in the foothills, and need to establish a strong base camp for the next challenges. To take one example: quantum computing will enable the analysis of much greater quantities of research data faster than can be done today, but it will also defeat current encryption systems, thus undermining privacy protections. Technical remedies will always be important, but solutions will ultimately be found in the moral and ethical principles we uphold in finding the way forward.

Baroness Neville-Jones is a member of Britain's House of Lords, and a former Minister of State for Security and Counter Terrorism