Think
new things
Make
new connections

Digital security for democratic, social and economic prosperity

A Ditchley Foundation conference, in coordination with Canadian Ditchley and the University of Ottawa

4-6 November 2022

DITCHLEY

Terms of Reference

Governments, societies and market economies are becoming increasingly dependent on data and digital capabilities, whilst geopolitical, technological and ethical digital security risks accumulate at pace. The open Internet, its core technologies and its multi-stakeholder governance model all emerged in a more benign context. Now, strategic geopolitical competition, political polarisation at home, runaway digital crime and AI all threaten to break the mould. There is also a tension between ever more digitisation, meaning ever more energy on Cloud servers, and sustainability objectives. What role should the private sector play in fostering digital security in ways that support democratic values and interests?

This Ditchley conference will gather leaders from across the private sector, government and non-governmental organisations to:

- Develop a fuller understanding of the different dimensions of digital security as the digital economy expands and matures.

- Explore the role of the private sector in the digital realm – alongside governments and non-governmental organisations – in protecting the stability of markets, the coherence of democratic societies and creating a sustainable global economy.

Questions arising

How do digital responsibilities for the private sector fit with the environmental, social and governance responsibilities that much of the private sector has already adopted as part of the purpose of a company? And, a linked question, will yet more responsibilities for companies, beyond shareholder value, accelerate the backlash against ESG (Environmental, Social and Governance) and "woke capitalism"? Should companies serve an ESG and democratic and digital security agenda?

Should the private sector be leading the debate on how best the evolving Internet should be regulated, aiming to influence government legislation and multi-stakeholder governance? Or should the private sector be mainly concerned with responding to legislation as it emerges?

To what extent, as with environmental concerns, should the private sector be getting ahead of legislation and acting to ensure environmental and social benefits in the digital realm?

How far can multinational companies operate across the Chinese and western spheres of influence of the Internet? To what extent should companies domiciled in the West see the promotion of democratic systems as part of their purpose and core responsibility?

How does the sharing of institutional digital risks and threats between companies and with government need to change, if overall network resilience and security is to increase? There seems to be consensus that the current practice of voluntary sharing of threats is not effective.

DITCHLEY

How does AI and the "metaverse" intensify and change the threat picture and responsibilities of companies?

Working Groups
For the middle part of the conference, we will separate into three working groups so as to be able to address sets of questions with more focus:

Group A: Private sector resilience and international competition
How can the values of the political West be sustained whilst also driving for a competitive edge in areas of the economy such as energy generation and supply, and in new sectors such as biotechnology? The war in Ukraine has exposed vulnerabilities for Western economies caused by the rapid growth of digitally based globalised economies over the last couple of decades. The vulnerability of supply chains, national security and energy security, for example, have all now been recognised as major blind spots. If there has been complacency over the degree and extent of considerations of resilience, how can this now be reversed? Have companies taken too narrow and inward looking an approach to resilience by concentrating only on their own operations, rather than their operating environment? How will climate objectives be recognised? Has the pressure from capital markets driven a far too short-term approach?

Group B: Changing nature of cybersecurity for the private sector
Cyber issues have now been elevated from IT issues to a major business risk with attacks growing in complexity and sophistication. What does winning the cybersecurity war look like? Around half of cyber attacks aim to steal money; the other half are targeted at data and are efforts to gain access and control. By sector, in 2021, healthcare was the most targeted – a sector with the most personal information (Investors Chronicle, 27 May 2022). Attack vectors and profiles are constantly evolving and include workforce behaviour. Artificial intelligence is a growing area, used both in attacks and in developing new forms of security. How will AI change cyber for companies? What is the overlap between cyber security, disinformation and other forms of covert influence such as "hack and leak" (where data is stolen in order to be released publicly and damage companies and governments)?

Group C: Driving international regulatory standards, norms and agreement
Data flows and the networks that enable them are becoming critical infrastructure for both companies and governments. What is the role of the private sector in supporting national governments and multi-national governance to work towards coherence, complementarity, enhanced synergies and to avoid regulatory fragmentation? Is privacy a major dividing line between democracies and authoritarian countries? Is it possible to create trusted data flows between democracies, yet alone between democracies and authoritarian states? How can governments, private corporations, companies and new entrants work together to create an international regulatory environment that enhances democracy, security and prosperity?

Background
The Internet (used as shorthand for the wide range of interlinked digital technologies that make up the modern world and global economy) delivers an extraordinary range of good things that is worth emphasising at the outset. A far from exhaustive list would include:

- Massively increased access to communications with friends, families, business partners, suppliers and clients.

- Massively increased access to educational resources and information.
- Much better access to information about health especially, saving lives.
- New markets and new business opportunities that have delivered great wealth for some and prosperity for many.
- New opportunities for art and creativity across music, film and new media.
- Accelerated innovation across many scientific and technological fields.

But, as we have now learnt, there are downsides too. Calls for greater safety and security are growing in intensity and many governments are preparing legislation. This is happening in an increasingly tense geopolitical context.

Modern digital security involves much more than the protection of computer systems against compromise by malware. At the most foundational level, there is the location, ownership and operation of the hardware. Whose cable network connects users to the Internet? Who built the switches? Who made and who operates the routers? There are concerns that a system built with Chinese hardware must be intrinsically insecure. The specific concern with digital security blends into a more general sense that democratic societies and economies cannot rely on infrastructure owned and developed by companies under the sway of hostile authoritarian regimes.

Resting on the hardware are the configuration and standards that make the Internet work. There is increasing concern that the current multi-stakeholder model of Internet governance is open to exploitation by organised and well-resourced authoritarian regimes, using effective small control to argue for sets of small changes that add to more than the sum of their parts. Meanwhile, a multilateral international model of governance with one vote for one nation (under UN auspices for example) is not attractive for democratic countries because of the risk of votes being traded, for example for Chinese Belt and Road investment. In the face of this impasse, there are at least two Internets in operation – a system open to all; and a system walled off from the West that rests on authoritarian principles with regard to data and privacy. This does not mean no privacy in authoritarian areas – companies are increasingly subject to quite stringent rules on data – but these rules do not constrain authoritarian states themselves, with China in particular continuing to develop its capabilities across the state for technological surveillance.

The division of the Internet into different zones is increasingly distinct with the general move towards the Cloud (hosting software operations and data on someone else's server). The location of Cloud servers determines the rules and regulations under which they are operated and who, and who cannot, gain locally legal access to the data. These trends are increasingly driving data localisation decisions (where data is kept within the jurisdiction of a government) and contributing to the concept of data sovereignty.

Beyond access to data conferred by standards, rules and local laws, there is the vast grey and fast developing field of clandestine and criminal access to data. Authoritarian countries' intelligence agencies are seeking access to data and operating systems not only at the level of individual companies and institutions but also through attacks on Cloud operating systems, Internet routers, cables and the Internet of Things. Some of these attacks are to gather confidential information, others are to prepare gateways for disruption in terms of tension of war, with there often being overlap between the two aims. Sometimes operating as proxies for government agencies, but also often just for profit, organised crime gangs are

ramping up ransomware attacks and other forms of digital extortion. The cybercrime 'industry' is becoming more professional and organised with ransomware malware offered as a service by criminal platforms, including helplines. Attacks are estimated to be growing at 60 percent per year and losses mounting. In the context of Russia's war on Ukraine, concerns are growing about attacks that might corrupt data rather than just lock it and disrupt markets; or malware attacks combined with attacks on hardware such as the cutting of submarine Internet cables.

Threats to the integrity, access and privacy of data are growing. These threats are not to the data alone but also extend to the functioning of sensitive systems that rely on the data, such as markets and industrial control systems. Threats and risks, therefore, like the systems themselves, are increasingly networked, with an attack on one part of the system potentially having consequences for other linked entities. Collateral damage is going to become increasingly common, with the implication that networks as a whole need to become more resilient and/or rapidly repairable.

Over and above security and privacy threats, there are risks to society from three directions.

The first is easy access to products or content that is either in itself illegal or is being accessed by children to whom its provision is illegal.

The second category is disinformation and the destruction of any certainty about the truth. This is happening on a domestic and international basis. Disinformation is in a close embrace with polarisation in democratic societies, with one leading to ever more of the other. Of course, people have always tried to assert their own version of the truth but the Internet has both industrialised and democratised this process, enabling many more actors to push out much more material, much more regularly. The result is a fog of lies and half lies. Foreign adversaries are able to exploit these conditions and use the same tools with the aim of intensifying polarisation and undermining confidence and clarity amongst electorates.

The third set of risks is more subtle and interwoven with Internet commercial business models. The Internet has arguably become a multifaceted machine designed primarily to attract attention for its advertisers, rather than to serve its users. This makes worse a range of ancient human maladies: the need for attention, vanity and jealousy for example.

The next generation of technologies to be folded into the architecture of the Internet will raise the stakes further:

The deployment of AI systems will conflate the risks of cyber security, privacy and disinformation, with potentially little transparency as to how decisions are being made and how data is being shared. Biases included in the training data or the structure of the AI model may be reinforced. AI is essentially an efficiency force and will change the nature of roles across many sectors, removing the need for some elements of work by human beings but creating others. No one knows how the mix will work out.

The development of augmented reality, virtual reality and the metaverse (whatever that turns out to be) is likely by its nature and business model to intensify the personal experience of the Internet and digital technology, with effects that are hard to predict, but that are likely to intensify the bad as well as the good.

States and multilateral organisations are addressing this cocktail of opportunities and risks according to their own strengths and interests.

The European Union, which does not have effective responsibility for cyber security which remains the preserve of European states as part of national security, is developing the most comprehensive package so far of digital legislation, to build on what is seen as the global success of the General Data Protection Regulation. This includes the Digital Markets Act, the Data Act and the AI Act. Officials privately acknowledge that there will be inconsistencies and unintended outcomes but see getting legislation on the table as overdue and urgent to contain current threats to EU citizens and markets. It remains to be seen whether the regulation can balance protection with a climate for innovation.

The UK and the US, with strong signals intelligence (Sigint) capabilities have focused more to date on protection from external Internet threats and have kept legislation relatively light, favouring innovation. Pressure is growing, however, to do something on privacy in the US and on damaging content in the UK, with the Online Safety Bill. The UK may produce its own lighter version of GDPR with the aim of enabling greater innovation and creating a better online experience for users.