Think
new things
Make
new connections

Conference Note

Digital security for democratic, social and economic prosperity

4-6 November 2022

A conference convened in cooperation with Canadian Ditchley and the University of Ottawa

DITCHLEY

EXECUTIVE SUMMARY

Governments, societies and market economies are increasingly dependent on data and digital capabilities and in a context of growing geopolitical, technological and ethical risks. What should and could the private sector do to improve their own digital security and the digital security of the markets and societies within which they operate?

This conference discussion reached the conclusion that, in the light of cyberattacks and the magnitude of their consequences, there is a decisive need to improve digital security and to put in place transparent regulation of the digital environment. Revision and modification can follow but now is the time to act. Alongside immediate regulation and a more active appreciation by the private sector of the fundamental values and benefits gained from operating within democratic societies, was a call for democratic societies to articulate a vision for digital states and digital citizens. What kind of digital environment will future citizens have and what can they expect from their state?

The shocks of the pandemic and Russia's war with Ukraine amount to much more than 'wake-up calls'. Cyber security is essential for all business operations – cyber risks are increasing in frequency and extend into a business environment increasingly shaped by intensifying economic competition. Existing standards, for example for an expanding set of IoT devices, have not prevented operation of their concealed business model which has led to the transfer of ever-growing quantities of data to competitor powers.

Disinformation and particularly misinformation were described as endemic, although there was debate about its scale and in the case of disinformation, the number of bad actors responsible. Either way, the prevalence of both reveals the degree to which the digital landscape is now a whole immersive environment or territory rather than a collection of discrete pieces of infrastructure.

In developing a regulatory response, there was agreement for a balancing of risks assessed across three main pillars – democracy, security and prosperity. To that end, ideas and recommendations were put forward. These included: a system of ESG standards for transparent data management (i.e. going beyond principles to action); a clear focus on the use of (and potential for switching off) recommender algorithms; government enforced access to data on disinformation from the major platforms to allow for a greater understanding of the problem and an ability to systematically target bad actors.

There was discussion of cyber rescue services aimed at providing help for smaller businesses and much more effort to be made to collaborate with technologically underdeveloped countries (such as sharing data sets and digital capabilities) to allow for their greater digital progress. Overall, the case was made for bringing together an established and maturing world of cybersecurity with the emerging but less well-developed communities to counter disinformation – whether through education, technological means or via emerging business models.

Inspired by the blue-ribbon committees in the US, there was a clear recommendation for some form of standing committees or commissions (complementary across countries) which could bring together digital resilience expertise from a range of sectors who are then empowered to make recommendations directly to governments for legislative change. This conference took place in Ottawa and was able to learn from considerable Canadian expertise and experience. The themes and

ideas discussed are core to Ditchley's ongoing work on technology, data and democracy and these will be integrated into the workstreams for 2023.

Context and why this was important

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?

People

An in-person conference with 41 delegates and 3 observers. Held in Ottawa with support from Canadian Ditchley and the University of Ottawa, this conference brought together interests across sectors and geographies and benefitted from the input and experience of representatives from the Canadian government under the chairing of The Hon. Sabi Marwah and Mr Calin Rovinescu C.M.

Analysis

FULL REPORT

The changing nature of cybersecurity for the private sector

The need for improving security is urgent and the time for action is now. The need for urgency comes from several sources: the rise of cybercrime; the use of information by adversaries to undermine democracy; the runaway innovation of transformative technologies and the difficulties governments have in responding; and a need to prepare for further disaster, whether caused by pandemic, conflict or climate.

Cyber threats are becoming ubiquitous and preventing them is a major business preoccupation. Canada reportedly experienced over 1bn cyber attacks per year. Malware is now a criminal business service and the barrier to entry is low. 60% of companies targeted by ransomware were said to have paid up. Cyber crime pays.

Geopolitical pressures add further complexity to digital security. US restrictions on semiconductor access for China, for example, and other export controls will change the ways business can operate. The introduction of laws that curb the scope of business is new. It seems unlikely that the US will loosen these restrictions in the short to medium term and they will limit Chinese companies, both in military and civilian fields. China's stance may also therefore harden. Other G7 countries have not yet taken such a securitized view but are under increasing pressure to choose sides.

Questions about the future picture of globalized trade follow. To what extent should allied countries be friend-shoring? What defines a friend? How will the trust necessary for trade be defined and engendered? There is a lack of trust at present between the US and EU on data protection. Can lack of trust even between likeminded democracies be bridged or are the underlying business philosophies just too different? And, how will these differences play out in the political relations between the EU and the US? Multilateral institutions such as the UN Security Council were not seen

as able to deal effectively with these diverging geopolitical philosophies. Even bodies such as the International Civil Aviation Organisation were said to be facing challenges in achieving regulatory harmony.

The combination of geopolitics and the need for regulation across different jurisdictions is creating new challenges for the private sector. Would new institutions be able to deliver regulation more effectively, and would they be able to do so without curbing opportunities of accelerating technologies? The observation that hard law is hard to enact whilst soft law is hard to enforce summed up the current situation. For many countries, GDPR (although it took time to embed) is now the gold standard and the EU AI Act (when it comes) may become a global standard. The US has no privacy law yet.

Other risks arising from the current moment of market competition include creating single points of failure. At present, tech markets tend to produce individual winners. The immense benefits, for example, of Ukraine's access to Space X's Starlink internet constellation is dependent on a powerful individual. Rather than corporations, individuals are the winners and they have unprecedent power. How can the resilience of governments, nations and indeed broader alliances be reliant on the willingness of a small number of extremely powerful individuals? The major corporations also have huge power and control over markets. The so-called 'hyperscalers' control much of the market and monopolize available human skilled labour. What should be the response from those countries who use (and rely on) but don't 'host' the major hyperscalers – that is, most countries other than the US and China? Should the G7 (or similar) insist on governance of the cloud security on which they depend?

The impact of emerging technologies on digital security

The emergence of the Internet of Things (IoT) and the convenience of a whole array of new internet linked devices has come at a cost of data loss. Huge quantities of data are now routinely transferred out of the country in which devices are used, to China. While an individual might not care whether information about them is collected or not, should the state care if this is being done to their citizens en masse? The number of IoT devices has increased from mundane household appliances to much more sensitive domains such as security cameras, smart toys or in medical treatments. In many instances, such transfer of data should not be taking place under existing regulations. There are standards for IoT devices. Products sold within the EU should conform to specific regulations, but how are regulations enforced and by whom? In some cases, these devices are simply breaking existing laws, but without consequence. Public awareness of such hidden business models is low.

Response to disinformation

Online disinformation received a lot of attention during this discussion. Studies that demonstrate the high speed at which deceitful information is spread compared with truthful information were highlighted. The optimistic take was that disinformation is now receiving the attention required and awareness of the problem has grown. However, such optimism is not enough. The case for proactive measures and greater deterrence was made. The emphasis should be on how to prevent rather than how to react.

But what action should be taken? Disinformation is not solely the propagation of factually incorrect information. Manipulation of fringe viewpoints funneled towards people already receptive to it, is a large part of the disinformation process. Such manipulation can not only influence people's opinions, but also influence their friendship circles as people build affinities with those who share their views.

This type of manipulation is hard to counter. It is not a simple case of improving digital literacy or critical thinking skills so that people can identify untruths.

The role of recommender algorithms in enabling manipulation was highlighted. Designed to serve content to keep people on the platforms, these are causing social and political damage. It was argued that these should have been switched off long ago, but of course the platforms aren't going to commit to doing so themselves, so who forces an intervention of this kind?

Analysis of disinformation is reliant on researchers and academics who track its prevalence and how the tradecraft is changing; they in turn rely on data from the platforms being available. This data tap is not guaranteed and may be turned off. The APIs that allow data to be transferred for analysis may not exist in future or may never exist on some of the newer platforms. Such data access cannot be allowed to disappear. The ability to switch off data streams cannot be left in the hands of the platforms themselves. Governments must ensure that data is available to people to research and uncover the extent to which disinformation is harming society.

Misunderstanding the scale of the problem

Much more needs to be done to substantiate the scale of the problem. There was challenge over the scale of disinformation in terms of the numbers of bad actors. It may be that much disinformation is delivered by a relatively small number of highly skilled experts. In terms of cybercrime, 95% of the problem is criminal groups, not state actors, and it comes down to a few hundred hackers based in places like Russia where they are free from worries of extradition. Counter measures have been taken. For example, in the run-up to the last US election, coordinated action against manipulation resulted in a dip in activity. Similarly, when Russia arrested various hacker groups, again there was a reduction in attacks. There are methods which have been successful but a more systematic direct response against bad actors is needed based on a better understanding of risks and evidence.

Addressing the dangers

Who do you call when you get hacked? Which law enforcement agency should be taking charge? This responsibility cannot be placed solely at the door of governments. The private sector needs to step up to ensure that their processes line up with policy. In the UK, the National Cyber Security Centre has the ability but limited capacity and mainly supports government or companies classed as critical infrastructure. There is also Action Fraud, or businesses can go to the National Crime Agency. How is the broader efficacy of these agencies to be assessed and where should limited resources best be targeted? Are citizens concerned by ransomware attacks on big businesses, as opposed to issues such as child sexual exploitation online? What role do traditional police services play? It was suggested that law enforcement in the digital domain is not working; it is a failure exacerbated by the lack of geographical link between the criminal and the victim and an inability to deal with cross-border crimes. Responsibility is bearing down on the private sector because existing law enforcement structures can't control these crimes and there is a lack of political will to carry out root and branch reform. Is this an area of state failure?

Education has a role to play if framed as part of a vision for digital states and digital citizens. What capabilities, equipment and infrastructure will future citizens have and what can they expect from their state? Education can be linked to a forward looking holistic vision of what it means to live in a digital society with democracy enhancing technologies, regulations and behaviours.

Driving international regulatory standards, norms and agreement

The challenge is to balance the overarching priorities of the digital landscape. What is an acceptable level of risk – we can have security or privacy, but cannot fully have both? Will society need to sacrifice a little more on privacy in order to maintain security?

This issue was framed in terms of three main pillars – democracy, security and prosperity – and the trade-offs that may need to be made between them. Would prosperity be the most-likely to be deprioritised in times of crisis and would the private sector agree? Does the private sector understand the primacy of democracies for keeping markets open? Progress on democracy-enhancing technology depends on the private sector being able to roll out developments at scale, which can only be implemented if all stake-holders come together to discuss what is needed. Such an endeavor must be pro-active and cannot simply be a means to counter existing authoritarian alternatives.

Progress is being made in terms of laws and regulations. Canada, for example, has several bills currently in Parliament or Senate, covering the regulation of online platforms, the availability of news content, cyber security and privacy. How such regulations will be enforced and how to penalise those who do not abide by them was an open question. A model of shared governance requires rules for cooperation.

Outreach to countries in the global south was considered part of this vision, but links between western countries and the global south have been badly neglected. Events in the south have the potential to shake western democracy. Meanwhile, China has dominated provision of digital systems to the global south. Huawei/ZTE dominate mobile internet infrastructure. Could data sharing partnerships be built and, if so, what datasets could be shared, for example, health or industry datasets? Digital development of the global south must be supported, and the transformative power of digital investment shared, especially the benefits of models founded on democratic principles. International standards for telecom standards and data sharing, for example, is simply not working well enough.

Quantum Computing

Dr Raymond Laflamme, Canada Research Chair in Quantum Computing at the University of Waterloo, gave a presentation on developments in the field of quantum technology since 2015, when patents for quantum technologies started to take off, with potential for improvements in such areas as health care, geological exploration and molecular imaging. The challenge for cryptosystems is that new algorithms that are quantum resistant will inevitably be required (post-quantum cryptography). Fifteen countries have developed national initiatives in quantum technology, investing upwards of $23 billion dollars. While it cannot be taken for granted that meaningful quantum computers will become reality, particularly while problems around the stability of hardware hold back improvements in performance, progress in the field is nevertheless underway.

Ideas for action

New commissions. Forward looking independent advisory panels. Inspired by the blue-ribbon committees in the US. With permanent but rotating membership these would bring together a diverse expertise to consider future digital resilience and competition in critical areas, for example information systems as a critical infrastructure for democracies or supply chains for key industries. Such commissions could be empowered to assess and categorise risk and make legislative

recommendations. Replicable at international levels, such commissions could promote greater resilience among like-minded nations. Could such a model allow mid-ranking liberal democracies in a broader alliance to work together? This requires government innovation planning and Five Eyes representation.

ESG ratings for data. One potential solution to low public awareness over the use of their data was to adapt models developed for ESG ratings and develop a rating system applied to the data realm. It was suggested that such an approach may force companies to be transparent about how they are managing their data.

Engaging the global south. Free provision of digital tools for data processing and for data centres. Work with industry and other leaders to offer and secure support. What privileged data sets can be can shared to support development and demonstrate the advantages of our values framework?

Government to support provision of cyber rescue services. Direct cybersecurity support for small businesses and start-ups who need more than advice. They require active help and support when attacked and to prevent attacks. NCSC to be involved.

Government to ensure the availability of data to allow for ongoing monitoring of the pathways and effects of disinformation.

Education to train children and every citizen to cope with digital traps, including disinformation. Civil servants, legislators, CEOs, teachers to be digitally educated. Greater permeability between legislators and technologists.

Preparing for pressures from decoupling, especially for the national security of middleweight powers (UK, Canada, Australia). These countries are currently dependent on US private platforms for cloud storage (Google, AWS, Azure). Can middleweight powers foster a greater diversity of supply to spread dependency and risk?

Industry-specific partnerships to create safe tools which serve the needs of specific sectors.

Collaboration beyond governments. Democratic societies tend to link organically at all levels: from the level of officialdom, between politicians, at the city-to-city level and at the citizen level. How can such links be maintained at different levels of society, even when the political leaderships doesn't agree?

The conference did not discuss the role of citizen activists such as Bellingcat, Vancouver's Citizen Labs, IIL, DFRLab and Ukraine's IT army. These kinds of initiatives have been critical in driving better transparency. What is the role of hacktivists in future?

The themes and recommendations made during this conference discussion will feed directly into Ditchley's 2023 Programme for Technology, Data and Democracy. Ditchley's programme will build directly on the connections made and the experience and leadership demonstrated by the Canadian government. In the first instance, the February conference on '*AI and creative destruction: how will current rapid advances in AI through large 'foundation' models impact on society, the economy and governments?*' will build on many of the issues raised in this discussion in Ottawa.

No participant is in any way committed to the content or expression given in this conference summary.

DITCHLEY

For a participant's perspective on this conference, the recommendations and outcomes see this reflection by Dr Kim Nilsson https://kimknilsson.medium.com/what-can-tech-do-to-further-global-digital-security-d6f944b1d15

Co-Chairs: The Hon. Sabi Marwah and Mr Calin Rovinescu C.M.

AUSTRIA

Dr Valentin Weber
Research Fellow, Technology and Global Affairs Program, German Council on Foreign Relations. Formerly: Open Technology Fund Senior Fellow in Information Controls, Berkman Klein Center for Internet and Society, Harvard University; research affiliate, Centre for Technology and Global Affairs, University of Oxford. PhD in cyber security (University of Oxford).

CANADA

Mr Guillaume Bazinet
Co-Founder, CEO and Chairman of the Board, FX Innovation. Chairman of the Board, Centre de Recherche Informatique de Montréal (CRIM).

Mr Serge Blais
Founder and Executive Director, Professional Development Institute, University of Ottawa. Formerly: Director of Student Academic Success Services, University of Ottawa.

Mr Stas Bojoukha CISSP, CISA, CISM, CEH, GSEC, COBIT
CEO and Founder, Compyl, New York.

Mr Andy Cheema
Consultant advising early-stage technology start-ups. Formerly: General Manager, Financial Services Ventures, Mattamy Ventures.
Ms Caroline Ford
Director, Democratic and Inclusive Governance Division, International Development Research Institute.

Mr Jacques Frémont
President and Vice-Chancellor, University of Ottawa; President, Québec Human Rights and Youth Rights Commission; Professor Emeritus, University of Montreal. Formerly: Director, International Higher Education Support Program, Open Society Foundations USA; Provost; Dean, Faculty of Law and Professor of Constitutional Law and Human Rights, University of Montreal. Member of the Program Advisory Committee, The Canadian Ditchley Foundation.

Mr Arjun Gupta
Director, Advisory Corporation Canada. A member of the board of Canadian Ditchley.

Ms Shreya Gupta
Technology, Privacy and Cybersecurity Associate, Norton Rose Fulbright Canada LLP.
Mr Jaxson Khan
Policy Advisor to Canadian Minister of Innovation, Science and Industry.

Dr Raymond Laflamme OC, FRSC
Jointly appointed at the Institute for Quantum Computing at the University of Waterloo, where he served as founding Executive Director (2002-17) and the Perimeter Institute for Theoretical Physics; Mike and Ophelia Lazaridis John von Neumann Chair in Quantum Information, University of Waterloo; Canada Research Chair in Quantum Information. Formerly: Director, Quantum Information Processing program, Canadian Institute for Advanced Research.

Mr Pierre Lortie CM, FCAE
Senior Business Advisor, Dentons Canada. Formerly: Governor, Council of Canadian Academies; President, Canadian Academy of Engineering; Bombardier (to 2003): President & COO, respectively, of: Bombardier Transportation; Bombardier Capital; Bombardier Intl.; President, Bombardier Aerospace, Regional Aircraft; Chairman, President & CEO, Provigo Inc.; President & CEO, Montreal Stock Exchange. Honorary Governor, The Ditchley Foundation; President, The Canadian Ditchley Foundation.

Ms Catherine Luelo
Deputy Minister, Treasury Board of Canada Secretariat and Chief Information Officer of Canada (2021-). Formerly: Senior Vice President and Chief Information Officer, Air Canada; Board of Directors, scale ai, Montreal.

The Hon. Sabi Marwah
Senate of Canada, appointed by the Governor General of Canada on the advice of the Prime Minister (2016). Formerly: Vice Chairman and Chief Operating Officer, Bank of Nova Scotia (Scotiabank).

Mr Don McCutchan
Director, Northstar Trade Finance; Senior Advisor, Navigator. Formerly: Partner and International Advisor, Gowling WLG LLP; Executive Director, European Bank for Reconstruction and Development. Vice-President and Secretary, Canadian Ditchley Foundation.

Mr Calin Rovinescu C.M.
Chancellor, University of Ottawa. Formerly: President and Chief Executive Officer, Air Canada.

Mr Guy Saint-Jacques
Senior Fellow, China Institute, University of Alberta; Fellow, Montreal Institute of International Studies; Fellow, C. D. Howe Institute, Toronto. Formerly: Global Affairs Canada (1977-2016): Ambassador to China; Deputy Head of Mission, Canadian Embassy, Washington DC; Deputy High Commissioner, Canadian High Commission in the United Kingdom; Government of Canada's Chief

Negotiator and Ambassador for Climate Change. Member of the Board of Directors of Canadian Ditchley.

Mr Mark Schaan
Senior Assistant Deputy Minister for Strategy and Innovation Policy, Innovation, and Science and Economic Development Canada.

Mr Allen Sutherland
Assistant Secretary to the Cabinet, Machinery of Government and Democratic Institutions, Privy Council Office, Government of Canada.

Mr Thomas Timmins
Partner, Lead - Energy Sector Group (Canada), China Executive Leadership Team and Chief Representative in Beijing, Gowling WLG, Toronto. A member of the board of Canadian Ditchley.

Mr Ray Williams ICD.D
Managing Director & Vice Chairman - Financial Markets, National Bank Financial. Formerly: Managing Director, Risk Management Solutions Group, Government & Institutional, Head & Managing Director , Institutional Derivatives Flow Sales, Managing Director, National Bank Financial. A Member of the Board of Directors, The Canadian Ditchley Foundation.

The Hon. Yuen Pau Woo
Senator (Independent) for British Columbia; member: Joint Standing Committee on the Scrutiny of Regulations; Standing Senate Committee on Foreign Affairs and International Trade; Standing Senate Committee on Banking, Trade and Commerce; member, Trilateral Commission. Formerly: President & Chief Executive Officer, Asia Pacific Foundation of Canada, Vancouver. Board Member, The Canadian Ditchley Foundation.

FRANCE/UK

Mr Robert Madelin
Chief Strategist, former Chairman and Director, Fipra International, Brussels. Formerly: UK and then EU public servant (1979-2016).

IRELAND

Ms Louise Burke FCCA
Managing Director, formerly Chief Finance Officer and Chief Operating Officer, Open Data Institute, London.

ITALY

Dr Paola Pierri
Director of Research and Design, Democratic Society, Berlin. Formerly: Research Fellow, Weizenbaum Institute.

SWEDEN

Dr Kim Nilsson
CEO & co-founder PeripherAi; founder, ex-CEO and now Chair, Pivigo, London; Entrepreneur of the Year, 2018. Formerly: Hubble Astronomer, Munich; Fellow, Max Planck Institute for Astronomy, Heidelberg.

UNITED KINGDOM

Mr Alex Creswell OBE
Senior Vice President for Government Affairs and Public Policy, Graphcore; Chair of AI and Digital, Manchester University.

Mr Gerald McQuaid
Director for Telecoms and Internet Security, Ofcom.

Mr Carl Miller
Founder, Centre for the Analysis of Social Media, Demos and CASM Technology.

Ms Nina Paine
Global Head, Cyber Partnerships, Standard Chartered. Formerly: UK National Crime Agency.

Mr Kalm Paul-Christian FRSA
Strategy Manager, Digital & Distribution, NatWest Group; Advisor, Chatham House. Formerly: Vice President, Financial Institutions Advisory, NatWest Markets (2018-22).

Mr Tom Plant
Founder and Principal, Liminal Minds Limite; Senior Associate Fellow, RUSI. Formerly: Director, Proliferation and Nuclear Policy programme, and Director, UK Project on Nuclear Issues.

Mr Richard Spearman CMG, OBE
Senior External Affairs Advisor for Security and Resilience, Vodafone Group.

UK/USA

Ms Kay Firth-Butterfield
Head of Artificial Intelligence and a member of the Executive Committee, World Economic Forum. Barrister, former Judge and Professor, technologist and entrepreneur; co-founder, AI Global; Vice-Chair, The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems.

/USA …

UNITED STATES OF AMERICA

Mr Kevin Allison
Vice President for Europe & Eurasia and Technology Policy, Albright Stonebridge Group. Formerly: Director, Geo-technology, Eurasiagroup, Washington, DC.

Mr Graham Brookie
Senior Director, Digital Forensic Research Lab, Atlantic Council. Formerly: positions at the White House and National Security Council, most recently, adviser for strategic communications.

Dr Corynne McSherry
Legal Director, EFF. Formerly: litigator, law firm of Bingham McCutchen, LLP.

Mr Adam Powell
Executive Director, USC Election Cybersecurity Initiative, University of Southern California (USC). Formerly: Senior Fellow and Director of Washington programs, USC Annenberg Center on Communication Leadership and Policy; Senior Fellow, USC Center on Public Diplomacy; member (and President 2015-19), Public Diplomacy Council of the United States; Vice Provost for Globalization, USC; Vice President for News and Information programming, National Public Radio.

Ms Lindsay Rodman
Visiting Associate Professor, George Washington University Law School. Formerly: Executive Director, Leadership Council for Women in National Security.

Ms Alexandra Seymour
Associate Fellow, Technology and National Security program, Center for a New American Security. Formerly: Chief of Staff to the CEO then as Public Policy Manager, CalypsoAI; speechwriter to the Deputy Secretary of Defense and as Senior Advisor to the Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats.

Ms Katherine Townsend
Director of Policy, World Wide Web Foundation, Washington, DC. Formerly: COO, data.org; innovation and transparency initiative, U.S. Department of State and the US Agency for International Development.