Whole of Government Digital Strategy
Dr. Taylor Owen

My recent work has focused on the implications of emerging digital technologies for state power and control. This work is summarised in a recent book *Disruptive Power: The Crisis of the State in the Digital Age* (OUP, 2015), and in two pieces particularly relevant to the The National Defence Review, The Violence of Algorithms in *Foreign Affairs* and Why Governments Must Embrace the New Global Digital Reality in *The Globe and Mail*. In short, I believe that the Defence Review should include a study of the wide range of digital policies and tools used across our foreign policy. Doing so will reveal some troubling contradictions in objectives and outcomes of these diverse initiatives, and point to the need for a whole-of-government digital strategy.

First, digital technology has enabled a new form of decentralized power in the international system.

Ten years ago, the following didn't exist: social networks, smart phones, the internet of things, AI, crypto currencies, silk road, drones, consumer virtual reality, 3D printing, mpesa, block chain, the Syrian electronic army, Anonymous, ISIS, Avaaz, Ushahidi, wikileaks. We can debate the individual importance, but taken together they tell us something interesting about a new layer of power in the global system.

- They are getting increasingly powerful. Quickly.
- Their power is at least in part dependent on technology
- They share a common set of emerging practices, norms and ethics
    - Formless, resilient, rapidly evolving, collaborative, etc.
- They are empowered in ways that sit outside of and in many ways challenge our 20th century hierarchical organizations – our international system.

Second, emerging technologies _also_ have a recentralizing effect.

This is occurring in two ways. First, states are using these same networks to try to re-establish control. Because of the behavior of perceived negative actors, both autocratic and democratic governments have chosen to treat the digital space as a battlefield. To as they say, "To collect it all, process it all, know it all." These policies include: Rapidly expanding the surveillance state; Vast international datasharing; Trying to break encryption; Unprecedented prosecution of whistleblowers and online crime; new limitations on free speech.

Second, power is being recentralized in the digital space through a new generation of high cost, large scale digital innovation, including: Quantum technologies; algorithmic governance, predictive policing; AI; autonomous weapons. These technologies concentrate power, in a handful of state and corporate power.

Third, despite this tension, those seeking control are fighting a loosing battle.

For four reasons.

- States have lost their monopoly on collective action. Command and control systems were once required to make large numbers of people do things. This is no longer the case.
- "States can't creatively destruct." Unlike in the private sector, government institutions can't be replaced by new organizations. They must evolve, which is a challenging proposition.

- Digital actors are empowered by the very “problems” that the modern nation state was designed to overcome (a lack of structure, instability, decentralized governance, loose and evolving ties). This means there is a disconnect between the structures and institutions that govern the international system, and the groups that increasingly have power.
- In the digital world, what enables the good, also enables the bad. In seeking to target perceived threatening actors, the state risks also shutting down all the positive benefits that the Internet and digital networks allow. In seeking to control, the state risk breaking the network itself.

What this means for Canadian Foreign Policy?

1. In general terms, which side of this divide do we want to be on?

Are we seeking to protect the network at all costs, and to support empowering technologies, or are we doing things that undermine its viability? For example, we can’t both support breaking encryption and use encryption to promote the speech of Iranian dissidents.

Are we taking dual use surveillance technologies as seriously as military weapons? In the production, sale and global deployment of surveillance tools, the state risks negating many of the positive steps it might otherwise be taking, online and off.

Should we be scaling back the surveillance state in order to preserve a single internet? What are the trade-offs of our participation in the five eyes surveillance network?

2. What are the new spaces of governance in which we could be acting?

What does a rules based system of norms and institutions to protect the freedoms and security of the individual look like in a world of rapidly evolving technological capacities? This will first and foremost require a rethinking the approach to online governance.

First and foremost, I think it means addressing the misalignment between our international institutions and the actors and technologies that currently have power. The status quo governance discourse delegitimizes many of the emerging actors with real power, and because of this it is blind to some of the core policy challenges of the 21st century.

Second, we need to look at what new technologies or socio-technological processes currently site outside of our international governance structures? Algorithms, autonomous weapons, quantum computing and crypto-currencies. What does governance of these look like?

3. How do we move beyond siloed digital foreign policies?

Put another way: What does a Whole of Government Digital Strategy look like? One that addresses together: surveillance, IP, C-51, dual use technologies, cyber war, autonomous weapon, online finance?