Digital technology has revolutionized everything, but government has much catching up to do, particularly in foreign policy. Adobestock photo

Towards a Whole of Government Digital Strategy

Taylor Owen

The world has changed drastically in the two decades since the advent of the internet, but our policy making and public discourse have failed to reflect the invisible shifts in global power distribution that have revolutionized politics, conflict, economics, social disruption and, as Taylor Owen writes, foreign policy.

Foreign policy was once the bastion of the elites. In military, diplomatic and humanitarian affairs, nation-states and the small group of individuals and institutions that governed their actions used primarily kinetic and broadcast channels to influence the actions of others. Control was largely exerted through hierarchical structures, and collective action through industrial organizations.

Digital technology has radically shifted this reality by flattening the operating environment in which global affairs is conducted. While nation-states of course remain powerful, the financial, political and ethical costs of controlling people and events are much higher. This digital shift has four consequences for Canadian foreign policy, that together require a rethinking of what it means to act and have influence in the world.

> *“Ten years ago, the following didn’t exist: social networks, smart phones, the internet of things, AI, crypto currencies, the Silk Road marketplace, drones, consumer virtual reality, 3D printing, mpesa, blockchain, the Syrian electronic army, Anonymous, ISIS, Avaaz, Ushihidi, wikileaks.”*

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, the Silk Road marketplace, drones, consumer virtual reality, 3D printing, mpesa, blockchain, the Syrian electronic army, Anonymous, ISIS, Avaaz, Ushihidi, wikileaks. We can debate their individual importance, but taken together they tell us something interesting about a new layer of power in the global system; a layer that shares some important characteristic.

> *“Policies that exemplify this desire for control and the extent states are willing to go to exert it include the rapidly expanding the surveillance state, vast international data sharing, efforts to break encryption, unprecedented prosecution of whistleblowers and online crime and new limitations on free speech.”*

Collectively, these tools and capabilities are getting increasingly powerful. Quickly. The trend is clear. While some technologies come and go, and impact can wax and wane, there is no question that decentralized digital capabilities are growing in significance. Faced with increased individual agency and potential for collective action, societies around the world have clearly chosen the messier economies and politics of decentralized tools. This power is at least in part dependent on technology, and these tools and groups share a common set of emerging practices, norms and ethics. They are formless, highly resilient, rapidly evolving, and collaborative. Finally, 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 seek to re-establish control over a world of empowered digital citizens. Because of the behaviour of perceived negative actors, both autocratic and democratic governments have chosen to treat the digital space as a battlefield. To, as they state in the Five Eyes surveillance collection posture, “To collect it all, process it all, know it all.” Policies that exemplify this desire for control and the extent states are willing to go to exert it include the rapidly expanding the surveillance state, vast international data sharing, efforts to break encryption, unprecedented prosecution of whistleblowers and online crime and 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 and autonomous weapons. These technologies concentrate power in a handful of state and corporate powers.

> *“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 and autonomous weapons. These technologies concentrate power in a handful of state and corporate powers.”*

Third, despite this tension, those seeking control are in my view fighting a losing battle.

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 when faced with the structural shifts enabled by digital technologies. 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. Finally, 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.

There are three major implications of this shift for Canadian foreign policy.

First, in general terms, we need to decide which side of this divide 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. They are morally and practically and strategically incompatible. Or, 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. Finally, 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? These are the types of question we need to start taking seriously. Not on the fringes of our foreign policy debate, but as fundamental challenges for reshaping our posture in the world.

Second, we should be asking, what are the new spaces of governance in which we could be acting? Our traditional global governance approach focused almost exclusively on elites and sought impact and influence in state-based international institutions. But 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?

> ***“Taking digital foreign policy seriously means moving beyond siloed digital foreign policies. The idea that surveillance policy, digital diplomacy, autonomous weapons development and digital humanitarianism can be discussed in isolated departmental silos is absurd.”***

This will first and foremost require a rethinking of the approach to online governance. 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.

It also means assessing what new technologies or socio-technological processes currently sit outside of our international governance structures. Algorithms, autonomous weapons, quantum computing and cryptocurrencies all exist in ungoverned spaces that fundamentally challenge the legitimacy and authority of the state. What does governance in this rapidly evolving space look like?

Finally, taking digital foreign policy seriously means moving beyond siloed digital foreign policies. The idea that surveillance policy, digital diplomacy, autonomous weapons development and digital humanitarianism can be discussed in isolated departmental silos is absurd. They all intimately effect each other, are based on the same data flows and algorithmic tools, and contradictions between them seriously harm our credibility and impact in the world.

Put another way: What does a Whole of Government Digital Strategy look like—one that addresses surveillance, IP, C-51, dual-use technologies, cyber war, autonomous weapons and online finance? Taking this question seriously, with all of the complexities it entails, is a pre-requisite for for any country seeking to engage with responsibility, legitimacy and continued relevance in the emerging global digital system.

Taylor Owen is Assistant Professor of Digital Media and Global Affairs at the University of British Columbia, a Senior Fellow at the Columbia Journalism School and the founder and Editor of OpenCanada.org. He is the author, most recently, of Disruptive Power: The Crisis of the State in the Digital Age *(Oxford University Press, 2015) and the co-editor of* The World Won't Wait: Why Canada Needs to Rethink its Foreign Policies *(University of Toronto Press, 2015, with Roland Paris). He serves on the Board of Directors of CIGI.*
His work can be found at www.taylorowen.com and @taylor_owen.
taylor.owen@gmail.com