Taylor Owen

2008 Trudeau Scholar

Columbia School of Journalism

BIOGRAPHY

Dr. Taylor Owen is the Research Director of the Tow Center for Digital Journalism at the Columbia School of Journalism. He is the Founding Editor of OpenCanada.org, the digital media platform of the Canadian International Council (CIC), is the Director of the International Relations and Digital Technology Project, an international research project exploring the intersection of information technology and international affairs, and is the Research Director of the Munk Debates. His Doctorate is from the University of Oxford where he was Trudeau scholar.

He was previously a Banting Postdoctoral Fellow at the University of British Columbia, a Fellow in the Genocide Studies Program at Yale University, a Research Fellow at the Center for Global Governance at the London School of Economics and a Researcher at the International Peace Research Institute, Oslo. His research and writing focuses on the intersection between information technology and international affairs. Taylor Owen's publications can be found on his website, at www.taylorowen.com, and can be followed at @taylor_owen.

ABSTRACT

Since the end of the Second World War, Canadian foreign policy has largely concerned itself with the promotion of individual rights and freedoms. This agenda began with Lester B. Pearson's insistence on the "Canadian clause" in the North Atlantic Treaty persisted through Canada's promotion of human security, and now finds expression in the government's rhetoric on the Arab Spring and its promotion of women's and gay rights internationally.

Until recently, Canada fulfilled its individual mandate by way of state-based international organizations such as NATO and the United Nations. States are, however, increasingly challenged by empowered individuals and groups. As a result, state-based institutions no longer possess the leverage to ensure the rights and freedoms of individuals.

How then does Canada as a state continue to promote the individual in a world in which states have diminishing power? This poses a challenge to foreign policy agendas, but also opens a new era of possibility, one in which the state works to protect the networks on which individuals empower themselves.

Disruption: Foreign Policy in a Networked World

The Department of English at the University of Denmark would seem an odd place to find provocative research on the digital era.[1] But it is here that a group of medieval historians, folklorists, and literary scholars led by Thomas Pettitt has developed a theoretical framework that goes a long way toward explaining our current, technologically enabled cultural shift.

The idea of the "Gutenberg Parenthesis" stipulates that we are now at the culminating moment of a revolution that will be complete when all cultural and knowledge production has been digitized—when all books ever written are digitized, all art reproduced, all news online. When this occurs—when our primary modes of interaction, communication, and production all *become* digital information—we will have ended a period of human history that was enabled by Gutenberg's printing press.

The printing press had wide-reaching consequences. In addition to allowing information to be dispersed widely, it also shaped how information itself was conceived. The printing press occasioned a

1. The author would like to thank Anouk Dey for his contributions to this paper.

shift from a chaotic, oral tradition to a linear, written one. If one wanted information to spread, one had to conform to a specific form, which was linear and bound, with beginnings, middles, and ends. Ideas were constructed to fit this form, and knowledge evolved via the constraints it imposed. Society moved from a decentralized, oral tradition of knowledge-sharing to information that could be centralized, controlled, and mass-produced.

These changes have largely determined the modern era. Some 350 years of governance, institutional design, political evolution, media, and culture have all been dictated by humankind's rapport with information technology. We are now adopting a new mode of information production, one based on digital information, with implications that are similarly destabilizing.

The Gutenberg Parenthesis is a useful lens through which to view the nature of contemporary threats and government responses. Pettitt would argue that the present and immediate security future will be marked by encounters, confrontations, and conflicts between pre-parenthetical illiterate individuals, parenthetical literate individuals, and post-parenthetical neo-literate individuals. In this construct, the pre-parenthetical insurgent and the post-parenthetical neo-literate will have more in common than the Westphalian security institutions. If this is true, then a contemporary discussion of foreign policy must move beyond the confines of state power, control and behaviour, and into the nebulous, networked world to which we have returned.

The Individual in Canadian Foreign Policy

Since the end of the Second World War, the individual has held a firm place at the centre of Canadian foreign policy. As much or more than any country in the world, Canada has justified its international presence in terms of the protection of individual security and rights and the empowerment of individual freedom.

While this position was made explicit with then minister of foreign affairs Lloyd Axworthy's human security agenda, it has been present through most of our major international initiatives spanning administrations of all political ideologies. And while it is true that all governments have deviated from this agenda in a range of ways, ultimately, Canada's role in the world for the past half-century has been rooted in the purported promotion of individual rights and freedoms. Tracing this history is illustrative.

The second of the 1949 North Atlantic Treaty's 14 articles is called the "Canadian clause" because it was introduced by Lester B. Pearson, then undersecretary of international affairs, who insisted that the parties of the agreement "should be bound together not merely by their common opposition to totalitarian communist aggression, but by a common belief in the values and virtues of…democracy and a positive love of it and their fellow men" (*Documents on Canadian External Relations*, 1949, 492). The Canadian clause emphasized the social aspect of cooperation and the individual.

Soon after the formation of the United Nations (UN), Canadian John Humphrey was named director of the Human Rights Division of the UN Secretariat, where he authored the Universal Declaration of Human Rights, the first time the individual was recognized by international law.

Meanwhile, the concept and practice of peacekeeping—an approach now seen in operations around the world—emerged from the Suez Crisis (1956), when Pearson developed the idea of a police force under UN control to separate warring parties. Of what is essentially a state-based concept, Pearson said that nonetheless "human sovereignty transcends national sovereignty" (Pearson, 1970, 14).

The human security agenda, too, is a literal manifestation of the promotion of the individual in Canadian foreign policy. In fact, former minister of foreign affairs Lloyd Axworthy originally referred to the human security agenda as the "individual security agenda"

(Copeland, 2001). As Axworthy explained at the UN, "the search for global peace increasingly turns on issues of personal safety…in this world, the protection of people must be central to the Council's work" (Axworthy, 1999a, n.p.).

The human security agenda saw tangible policy success. The Kimberley Process and the UN Doctrine on the Responsibility to Protect both owe their provenance to the concept of human security. Similarly, Canada's policy toward Kosovo was articulated in terms of the human security agenda. "It was and is the humanitarian imperative that has galvanized the alliance to act…NATO's actions are guided primarily by concern for the human rights and welfare of Kosovo's people," explained Axworthy (Axworthy, 1999b, n.p.).

The Anti-Personnel Mine Ban Convention, in which Canada played a formative and lasting role, was also very much seen as an accomplishment aimed at protecting the individual. At the signing of the treaty, Axworthy explained, "An independent and effective international criminal court will help to deter some of the most serious violations of international humanitarian law. It will give new meaning and global reach to protecting the vulnerable and innocent" (Axworthy, 1998, n.p.).

Another example can be found in Axworthy's announcement of the creation of the International Commission on Intervention and State Sovereignty as a response to Secretary-General Kofi Annan's call for new ways of addressing complex international challenges such as the Rwandan genocide and the Srebrenica massacre. "Canada's human security agenda is all about *putting people* first [emphasis added]," Axworthy said, and "we are establishing this Commission to respond to the Secretary-General's challenge to ensure that the indifference and inaction of the international community…are no longer an option" (Axworthy, 2000, n.p.).

The mission in Afghanistan, which was initially clearly about supporting an American-led regime change, was depicted by all governments as having a humanitarian imperative. Throughout the

mission and the evolution from 3D, to Whole of Government, to Integrated Peacebuilding, the protection and promotion of Afghan security, broadly defined, was rightly or wrongly at the centre of governments' public rhetoric.[2]

The omnipresence of the individual has transitioned into the Harper government's foreign policy. When the Libyan government first started attacking its citizens, Prime Minister Stephen Harper stated, "Canada urges Libyan forces to respect the human rights of demonstrators, including their right to freedom of expression and assembly" (Harper, 2011a, n.p.). A month later, he continued, "We must help the Libyan people, help them now, or the threat to them and the stability of the whole region will only increase" (Harper, 2011b, n.p.). More recently, Minister of Foreign Affairs John Baird has made forceful statements on women's and gay rights. The "criminalization of homosexuality," Baird recently stated, "is incompatible with the fundamental Commonwealth value of human rights" (Davis, 2012, n.p.).

What is important to note about this evolution is that for 50 years, Canada has promoted the rights and freedoms of individuals through state-based multinational organizations. Over the past decade, however, these institutions have proved wanting at fulfilling the mandates they were built to advance. The list of recent multilateral policy failures is sobering: Afghanistan, Iraq, Kyoto, nonproliferation, and any number of macro development initiatives.

If the human security agenda taught us that state sovereignty is insufficient for protecting individual security, an assessment of the current international system must surely add that networked individuals are now empowered both to protect and to harm themselves. The state is increasingly left out of both sides of the equation.

2. 3D refers to Diplomacy, Defence and Development. All three terms where used during the mission in Afghanistan to refer to government departments coordinating both at the headquarters level in Ottawa, and at the operational level in the field. They imply that military, development, and diplomatic tools are required in a peacebuilding mission.

How then does Canada as a state continue to promote the individual in a world where states have diminishing power? This poses a challenge to foreign policy agendas, but also opens a new era of possibility, one in which the state works to protect the network through which individuals empower themselves.

Anonymous

In all areas of international affairs, some of the most successful contemporary actors are those that are leveraging online networks to disrupt traditional institutions. Perhaps none better exemplifies this than the activist collective Anonymous.

In the summer of 2010, under pressure from the US State Department and in response to the WikiLeaks release of hundreds of thousands of diplomatic cables, MasterCard, VISA, and PayPal halted all donation transactions to WikiLeaks. Soon after, all three of their sites went down due to an online attack, called Operation Payback, by the activist group Anonymous.

Anonymous was able to shut down three of the biggest financial sites on the Internet using a distributed denial-of-service (DDOS) attack. A DDOS shuts down a site by overwhelming its server with a large number of simultaneous activities. This is generally done using a low orbit ion cannon (LOIC) program that leverages a single network connection to send a firehouse of garbage requests. A LOIC program allows people to participate in a collective hacking initiative without knowing how to program.

Anonymous defines itself as a "decentralized network of individuals focused on promoting access to information, free speech, and transparency." Starting in 2008, the collective began to retaliate against the anti-digital piracy campaign of the motion picture and recording industry. Since then, hundreds of attacks have been conducted under the Anonymous brand. Throughout 2011, Anonymous attacked the government websites of Syria, Egypt, and Libya in support of the Arab Spring. In January of 2012, Anonymous hacked into,

recorded, and made public conference calls among agents of the FBI and MI5 who were meeting on how to stop cyber-activism. Personal details have been released of the police officer who pepper-sprayed protesters at the University of California, San Diego, and of Arizona lawmakers who brought in state anti-immigration laws. In April 2012, Anonymous broke into the computer networks of the Vatican.

Anonymous has no centralized leadership and no country of origin. Individuals loosely coordinate, and apply the Anonymous label to their action as attribution. As one self-identified Anonymous hacker put it, "We have this agenda that we all agree on and we all coordinate and act, but all act independently toward it, without any want for recognition. We just want to get something that we feel is important done."

In a recent *Foreign Affairs* article, Yochai Benkler, professor at Harvard's Berkman Center, argued, "Anonymous demonstrates one of the new core aspects of power in a networked, democratic society: individuals are vastly more effective and less susceptible to manipulation, control, and suppression by traditional sources of power than they were even a decade ago" (Benkler, 2012).

Members of Anonymous are neither pranksters nor terrorists, Benkler continued. Instead, they "play the role of the audacious provocateur, straddling the boundaries between destructive, disruptive, and instructive" (Benkler, 2012) Like many of the individuals and organizations innovating online, they confound the institutions, boundaries, categories, and actors that have held power throughout the 20th century.

Leveraging the Networked Architecture

If the new international architecture is an environment in which threats are focused on people rather than on states, and the power to cause and mitigate harm is decentralized to individuals, then understanding the networks within which individuals act becomes a central foreign policy prerogative. Networked actors are no more

morally bound than actors that operate within the traditional state system. They use their power for both positive and negative acts. It is therefore their ability to act, and the new forms of action that are enabled by networked technology, that should be the focus of our study.

While Anonymous is by no means representative of all networked organizations, it is an archetype of a new type of institution—one that has proved remarkably successful. For this reason, Anonymous is a useful case study for online networked behaviour.

Technologically enabled

The principal characteristic of the networked world is the individual enabled by information technology. Instead of seeing advances in how we communicate, broadcast, and interact as an incremental evolution, we can see the Internet, and the norms and practices that it enables, as instrumental to a wide range of behavioural shifts. Because of information technology, the individual is now empowered in a manner that challenges the institutionalized structures of global affairs.

In a study of the online "blogstorm" response to the anti–John Kerry "swift boat" documentary *Stolen Honor*, legal scholar Marvin Ammori argues that the primary variable in the ability for political action that has shifted is the barrier to entry. Marginal production and distribution costs are now so low that online participants are able to overcome the technological and logistical costs and the organizational barriers to coordinated political action (Ammori, 2005, 43-46). This ability for ad hoc collaboration enables a network of individual participants driven by non-monetary motivations (Ammori, 2005, 50) and leverages their excess labor capacity (Ammori, 2005, 55).

To this factor, Michael Froomkin adds the inherent value of anonymity to explain the growing power of the individual in an online

network. It is a technologically determined anonymity, he argues, that allows individual users to engage in political speech without fear of retribution and, as such, gives them power (Froomkin, 1997).

Self-governed

If the Internet technologically empowers individuals to act on their own, how does it regulate collective behaviour? Ammori argues that collective action in what he calls a "blogstorm" is self-regulated. He argues that technology is enabling a new form of "collective ad hoc private regulation," whereby private actors deliberately constrain and influence other private actors (Ammori, 2005, 3). Ammori calls this self-regulation "shadow government," a term perhaps drawn from law and economics theorist Robert Ellickson, who describes actions "within the shadow of the law" (Ellickson, 1991). Lawrence Lessig also argues that the legal control of behaviours is just one of many forms of constraints, including norms, markets, and system architecture. So the fact that a network is largely lawless does not mean that it is unregulated; it simply means that it is regulated by alternative (private) means (Lessig, 1998).

In 2002, Yochai Benkler adapted this idea of self-regulation to the Internet age. Benkler builds on the theory of Robert Coase, the father of the discipline of law and economics, which classified the regulation of interactions as either market-based (via contracts) or hierarchy-based (via institutions), to posit that the Internet permits a third model of production: ad hoc volunteerism (Benkler, 2002).

In this governance system, credibility and authority are gained through action. In a lovely turn of phrase, Sundén says that on the Internet one "types oneself into being" (Sundén, 2003, 3). Similarly, in *Communications Power*, Castells argues that the new actors gain their power from communication, not from representation (Castells, 2000). Both imply that authority in online networks such as Anonymous is judged only by the reality the participants create.

Polysocial

Sally Applin and Michael Fischer argue that we have reached the end of the singular perceived self and that we now exist, online and offline, as multiple identities in multiple simultaneous realities (Applin and Fisher, 2011). This "polysocial" reality not only encompasses the seamless blending of real and virtual worlds, but also reflects the multiple and simultaneous realities in which we choose to live. These realities are at once personal and anonymous, and we are increasingly seeing a tension between the two. We now can exist in multiple places at once and are in this sense becoming ubiquitous.

It may be, as Catherine Fieschi has written, that this reality involves a completely different way of thinking, a neurological rewiring (Fieschi, 2011). Neuronal plasticity posits that humans are malleable and that their nervous system can adapt. Jonah Lehrer, for example, argues that interaction with diverse actors improves our mental acuity for problem solving (Lehrer, 2012). In this sense, we could well be nearing the end of the "modern self," that is, the self-contained, self-reflective, and isolated individual.

Which identities people assume and which they choose to be a part of is the purview of behavioural economics. One idea particularly relevant to networked online activity is homophilous sorting: the process by which individuals come to identify and preferentially interact with those similar to themselves. Timar Kuran describes what he calls preference falsification within self-selected groups, which predicts that a community might be attached to a status quo belief even if none of its members individually support it. In these social networks, individual actors refrain from expressing their discontent or preference for change in order to avoid punishment (Kuran, 1995). Behavioural economists also show that when an information consumer is uncertain about the quality of a source of information, he or she infers that the source is of higher quality when it conforms to their previously held biases (Gentzkow and Shapiro, 2006).

Rapidly evolving

In a digital network, information is abundant and evolves at an increasingly fast pace. News of world events has become a commodity, and the evolution of ideas, ideologies, beliefs and politics is nearing real time. Software programs, group behaviour, and individual action are all adapting to a world of big data and a new pace of evolution.

The scale of data now being produced is incomprehensible to the human mind. For example, we produce a Library of Congress worth of data every five minutes. Much of this data is meta-tagged and social; two billion pieces of content are tagged with a location on a monthly basis on the Facebook platform. This flow of data is leading to a new law of production, where the more we consume, produce, and use data, the cheaper it becomes—data is not subject to resource constraints.

This scale and pace of information production is leading to changes in how individuals behave. Ammori argues that in online networks, relationships are less likely to be grounded in history. The implication is that group loyalty does not ensure path dependency. In the Sinclair case (outlined above), the blogstorm lasted "only one and a half weeks, and it even appeared to lose vigour after only its third day" (Ammori, 2005, 26). It created no permanent institution (Ammori, 2005, 28) and, when another broadcaster committed precisely the same action, it received no attention (Ammori, 2005, 29).

Marketing theorist Seth Godin's book *Unleashing the Ideas Virus* argues that online, certain ideas can take on a life of their own, acting like viruses and self-marketing. Similarly, J.M. Balkin suggests that messages act like "memes"—viral ideas that use people to replicate themselves (Balkin, 1998). This biological evolution is also iterative. In the Sinclair case, each time the stock of the company that produced the video went down a few cents, bloggers would circulate the information and the stock would fall further (Ammori, 2005, 21).

Internet theorist Evegny Morozov argues that online networks, and the pace of change they enable, lead to a motivation to engage in superficial forms of politics (2011), where individuals are incentivized to behave loudly and assertively.

Decentralized, non-hierarchical, and collaborative

Action in a networked environment is not only data-heavy and rapidly evolving, but is both decentralized and non-hierarchical. More importantly, collective action is possible without centralization and a hierarchical structure. Clay Shirky argues that collective activities that formerly required coordination and hierarchy can now be carried out through looser forms of coordination (Shirky, 2010), such as social network connections, common short-term alignment in a movement, or unified objectives in a particular event. Drawing on game theory, Ammori argues that decentralized action allows participants to overcome perceived or real collective action problems such as the Prisoner's Dilemma and Chicken (Ammori, 2005, 39).

In *Smart Mobs: The Next Social Revolution,* Howard Rheingold makes the case that the power of the network is largely quantitatively derived (i.e., derived from its population). Rheingold compares this with a state, where population does not automatically deliver power. According to Rheingold, networked power follows Reed's Law: a network's power increases by the square of the number of its members, so new members increase a large network's power more than they would the power of a small network (Rheingold, 2002).

Writing about networked governance, Mark Considine argues that a network is a social world based upon partnerships, collaborations, and interdependencies, as opposed to command-and-control hierarchies, market exchange, and traditional bureaucratic instruments (Considine, 2005). Manuel Castells adds that networks enable a new collective capitalism, the "signature form of organization in the information age" (Castells, 2000, 57). Bruno Latour introduces

actor network theory, which sees collaboration as lateral encounters and a key feature of the network (Latour, 1997).

Networked action and the decentralized nodes of Anonymous are not geographically predicated. Clay Shirky, for example, demonstrates that the Internet unites groups so disparate that they could not have been formed without it (Shirky, 2008). Hargittai argues that online segregation is based not on geography but on other factors like nationality, age, and level of education (Hargittai, 2007).

Resilient

Computer scientists have long studied the resilience of networks. A recent article in *Nature*, however, argues that not all redundant networks are equal. The authors show that one attribute of scale-free networks, such as the Internet, is that most of the network's nodes have one or two links; few nodes have more. This guarantees that the system is entirely connected and is therefore particularly robust. More specifically, the ability of nodes to communicate with one another in networks such as the Internet is unaffected by high node failure rates, giving these networks a high tolerance for error and ensuring that they continue to grow even when a small error occurs. This tolerance for error comes at a high price, however: if key nodes are attacked, the entire network becomes vulnerable (Albert et al., 2000).

The Internet's resilience follows not only from its high tolerance for error but also from its packet-switching characteristic. Cyber law scholar Michael Froomkin (1996) describes packet-switching as the method by which data can be broken up into standardized packets, which are then routed to their destinations via an indeterminate number of intermediaries. Having so many possible routes for communication means that information can still be transmitted when one break occurs. This is one reason why the US Department of Defense developed the Internet.

Social

In the field of international relations, social behaviour is intimately associated with constructivism. "Actors do not have a 'portfolio' of interests that they carry around independent of social context," writes Wendt. "Instead, they define interests in the process of defining situations" (Wendt, 1992, 398). In the online environment, many of the same dynamics are at work. Danah Boyd argues that MySpace and Facebook allow US youth to socialize with friends even when they are unable to gather in unmediated situations, thus serving the function of "networked publics" that support sociability (Boyd, 2008). Haythornthwaite argues that because individuals can articulate and make visible their social networks, individuals with "latent ties" can make connections that would not usually be made (Haythornthwaite, 2005). Clay Shirky goes a step further, arguing that peer-to-peer is "erasing the distinction between consumer and provider" (Shirky, 2008, 35) and creating new forms of socio-economic relationships.

Principles of Foreign Policy in a Networked World

Governments and their foreign policy agendas are faced with a dilemma: the very attributes that determine success in a networked world (outlined above) are the ones that their institutions were built to dissuade.

In a world where states had a monopoly on power, it was sufficient for the state to use state institutions to protect and empower individuals. But this is no longer the case. In the online space, where individuals are empowered by networks, the only choice for the state is to determine ways of mitigating the potential harms of networked behaviour, and using the state's political, economic, and regulatory powers to incentivize behaviour that is broadly in its citizens' interests.

Solving this dilemma is a project far beyond the bounds of this paper, but four principles underlie how the individual can remain at the centre of Canadian foreign policy in a networked world: to

embrace disruption, to protect the network, to support empowering technologies, and to build online literacy.

Embrace disruption

Legacy hierarchical organizations are at a crossroad. Information technology and networked organizations both challenge and disrupt their very existence. These organizations were quite simply designed and built for a different world. In the case of organizations that are private corporations, such as newspapers or auto manufacturers, then creative destruction may very well be a net positive. Creative destruction is more difficult, however, in the public sector. Foreign ministries, militaries, and intelligence agencies are not going to simply disappear and be replaced by start-ups. The new information environment, however, may require them to adopt some characteristics of start-ups. The challenge for government is how to rebuild, reform, reimagine, and disrupt its own institutions in order to remain relevant and to function in a digital era.

One idea, suggested by Catherine Fieschi (2012), is instead of simply moving our old institutions online, to do the opposite and look to successful online forms of communication, action, and organization to see if we can scale them up or use them as models for new institutions.

While this sort of wholesale reengineering is currently nowhere to be seen, there are small signs of evolution. The US State Department has led the way in using social media to actively engage global actors. It runs a wide range of experimental programs in the technology space, which are possible only because of a cultural shift toward high risk acceptance. It has begun the process of legitimizing a new form of organization.

Examples of very small steps in this direction in Canada exist as well. Foreign Affairs and International Trade Canada has begun talking about new ways of organizing through its Open Policy initiative. The challenge is that being truly open is very difficult for an

organization in which ambassadors—let alone desk officers—are not allowed to speak publicly.

Other branches of foreign policy are going in a direction that could lead us to a very different place. As pointed out by Ron Deibert (2011), the director of the Canada Centre for Global Security Studies and the Citizen Lab, the United States now considers cyberspace a "domain" equal in importance to land, sea, air, and space. Diebert cautions that we may be headed to a place where states seek to control more and more information, rather than to enable its free movement—a world of more state control and surveillance, a nanny state run amok. Reverse engineering the online world would take us in the opposite direction, one where the state's presence online is enabling, rather than punitive.

Writing in *Foreign Affairs*, Benkler argues that the United States has begun to see Anonymous as a national security threat. The problem with this approach is that it imposes a state-based structure on what is an "idea, a zeitgeist, coupled with a set of social and technical practices" (Benkler, 2012). Policy-makers would be wise to instead see Anonymous as a model for power in an alternative system and as a constructive mode for new frameworks of engagement and organization. The model that Anonymous represents is disruption.

In international affairs, the term "rogue" is typically used to describe states that operate outside of the rules of the game. These states do not follow the norms of the international system. Similarly, Anonymous does not use the accepted international architecture to oppose the state. Its power is rooted in the community with which its members are connected, and in many cases it operates in a fashion that challenges the authority of both democratic and autocratic state institutions. But while a rogue actor seeks to destroy the status quo, actors who are described as "disruptive" also pursue political and social justice. Yochai Benkler argues that unlike Al Qaeda, another powerful distributive rogue network, Anonymous "causes disruption, not destruction" (Benkler, 2012). It is through network-enabled

disruption that Anonymous seeks to disrupt the economic and political systems developed over the past century. As cybercrime author Richard Power observes, it is "attacking the whole power structure" (Sengupta, 2012).

Josh Corman argues that Anonymous demonstrates that "those who can best wield this new magic are not nations. They're not politicians. The youngest citizens of the Net don't even recognize allegiance to a country or to a political party. Their allegiance is to a hive. In some ways this is very exciting. In other ways this is terrifying" (Gross, 2012). State institutions simply must embrace disruption if they are to be relevant in a networked world.

Protect the network

If a government cares about protecting and empowering individuals, then protecting the freedom with which they engage online should be a focal point of its foreign policy. This year, the international community will renegotiate the UN treaty concerning the governance of the Internet. On one side of the negotiations, the United States and its allies want to keep the Internet run by a small group of non-profit organizations based in the United States. On the other side are states, including Russia, China, Brazil, India, and Iran, that want a new global body to oversee the Internet.

States in both groups, however, have used a wide range of the same intrusive monitoring technologies against their own citizens. Indeed, both groups of states oppose having the actor at the negotiating table—by "actor" we mean those individuals and groups that exist on and make up the online network. We are left with a state-based institution negotiating how individuals will use a network run by individuals.

What would a state's policy toward the Internet look like if it were to embrace the voices, values, and attributes of those that live in the networked world? What if a foreign policy were to seek to protect the very foundation of the system that powers the 21st century?

As essayist Michael Gross describes the Internet negotiations, states "want to superimpose existing, pre-digital power structures and their associated notions of privacy, intellectual property, security, and sovereignty onto the Internet." Online-born actors, groups, and institutions would instead "abandon those rickety old structures and let the will of the crowd create a new global culture, maybe even new kinds of virtual 'countries'" (Gross, 2012).

This is already occurring. Even as UN negotiations seek to regulate the Internet's Domain Name System (DNS), new parallel systems are being developed. The latest is called the Open and Decentralized DNS (ODDNS) and is based on a peer-to-peer network that openly shares both the domain names and related IP addresses of its users. Its creator, Jimmy Rudolf, says he built the system to "show governments that it is not possible to prevent people from talking" (Torrentfreak, 2012).

A hacker that Gross interviewed puts it well: "The more government tries to regulate, the more people will try to build an Internet that is uncensorable and unfilterable and unblockable." They will circumvent state control. And, again, therein lies the paradox that legacy state institutions face. The online information network has certain characteristics that run directly counter to the structure of state institutions. Its borderlessness, its propensity for information to be free-flowing rather than protected by copyright, its ability to preserve both greater anonymity and near-complete transparency—all are antithetical to traditional state control.

Even worse, as Benkler eloquently states, fighting against this tide will put governments "at odds with some of the most energetic and wired segments of society." This has real policy consequences: "Any society that commits itself to eliminating what makes Anonymous possible and powerful risks losing the openness and uncertainty that have made the Internet home to so much innovation, expression, and creativity" (Benkler, 2012).

Support empowering technologies

At the centre of the Internet's freedom agenda lies a paradox: the tools that enable autocratic governments to monitor and control their citizens are produced by Western technology companies. Much like the arms trade, this often creates the awkward scenario in which Western countries are supporting opposition movements that are fighting against technology bought from Western countries.

The Citizen Lab at the University of Toronto has uncovered a wide range of examples of complicity between Western companies and authoritarian regimes. Most recently, it showed that devices manufactured by Blue Coat Systems, a California-based hardware company, were being used in Syria to both censor the Internet and root out particular activities linked to pro-democracy activists (Deibert, 2011).

This same type of commercial filtering and monitoring technology is used by Western governments, including the Government of Canada and our Department of Foreign Affairs and International Trade, to monitor and restrict the online behaviour of its employees. This opens the real potential that Western governments are supporting private companies that develop technologies that assist the oppressive regimes opposed by our governments.

Indeed, if one were to attend a trade show for such technologies, as a *Washington Post* journalist recently did, one would find more than 35 US federal agencies buying the very same technologies as the autocrats (Horwitz, Asokan, and Tate, 2012). The US State Department, which has spent $70 million promoting Internet freedom abroad, is part of a government that has no regulation on the trade of the technology that prevents such freedom. A bill has been before the US Congress to restrict the sale of this technology to "Internet-restricting countries" since 2006, but the implementation of this bill may be challenging, as the list of countries in question now includes most nation-states.

Technologies that can be used for both positive and negative impact pose a challenge. For example, even as the US government funds Commotion Wireless, a sophisticated hacking project that seeks to enable activists by undermining Internet censorship in countries such as Syria and Iran, the FBI recently warned that these same anonymizing and encryption tools might be "indicators of terrorist activities" (Burkeman, 2012).

The question for policy-makers is therefore whether this hypocrisy can be reversed or whether it is simply a fact of life in a radically open operating environment. Whatever the reply, a relatively simple place to start would be to support the development of technologies that empower individuals rather than enabling the production and trade of tools used for surveillance and oppression.

For example, a Swedish research team recently developed a new tool that allows Tor communication (Tor is a tool that anonymizes Internet use) to be cloaked within services like Skype in order to circumvent recent changes to the Chinese "firewall" that had compromised those who used Shype. This is clearly an act of foreign policy and one that governments should support. One can even imagine a virtual embassy incentivizing such projects.

Build online literacy

In the new information technology world, literacy has taken on a whole new meaning. It is no longer enough to train our citizens to read, write, and do basic math. They need to become digitally aware citizens, cognizant of both the content they are consuming and the technology that underlies it. This means that they need much better critical thinking skills to judge credibility, accuracy, and authority.

Citizens must also understand the physical and software infrastructure on which the digital information world is built. This means knowing how algorithms deliver the news, how open-sourced editing works, and how the demographics and biases of computer programmers affect the world in which citizens engage. Ultimately, this

will require widespread basic computer programming to be taught like any other language.

Empowering the Individual

The international system has always been a network of states and individuals. At varying times over the past century, we have seen different alignments of state and individual power and problems. In the interwar period, while the state system was strong, we largely saw individuals negotiating solutions to state-based problems without the support of their countrypeople, resulting in fragile agreements. In the postwar period, there occurred a successful matching of powerful and legitimate state actors, multinational organizations, and transnational corporations addressing what were state-based problems.

In the contemporary era, states are still seeking to exert power and influence through 20th-century institutions even as the problems and the principal actor have shifted to the individual. Moreover, the very system in which international affairs is conducted has shifted from a state system to a networked world.

The core question therefore becomes, What is the role of the state in a world where individuals are increasingly empowered to negotiate solutions to individual problems? For Canada, this question represents a unique opportunity. For the first time since the individual took centre stage in our foreign policy, we have at our disposal mechanisms to empower him or her.

This empowerment will mean moving away from state-based institutions such as international organizations, large state-based development assistance, and multinational military occupations, into the nebulous, ill-defined, quickly evolving networked world. Perhaps even more challenging, it will mean rethinking the state institutions through which we have conducted foreign policy for over a century.

It is worth noting that a network freedom agenda is tailor-made for a Conservative government. The agenda combines many of the principles Conservatives espouse, including individualism and the promotion of democracy, and it moves away from the multinational organizations Conservatives have long questioned. Perhaps most importantly, the agenda could form the grounding of a modern human rights agenda, which the Canadian public has long seen as a core attribute of Canada's foreign policy.

Exploring Canada's role in a networked world is a complex and problematic task and one for which the disciplinary silos of academia are profoundly ill-suited to address. For this reason, it fits perfectly within the mandate and capacity of the Trudeau Foundation. The Foundation could support research that addresses the central challenges and problems of networked international affairs. Following are examples of relevant research areas:

Behaviour: The Foundation could support research into how individuals and groups behave in a networked environment. This would include everything from assessing motivations, to evaluating the structural determinants of positive and negative actions and outcomes. What is driving change in a networked system? Do networks create social relationships that are neither hierarchical nor market driven? In what ways can the state act to complement the actions of individuals? What mechanisms allow contemporary actors to leverage networks that disrupt traditional institutions?

Structure: A second set of research questions could explore the structure of networks themselves. This would seek to gain a better understanding of the design of the architecture that underlies the network. How do we separate network theory from network analysis tools? How do we assess the relational influence and power of actors in a network? What analytic categories can help us distinguish different types of networks in the international system? What meaningful communication patterns exist between actors in a network?

Ethics: Do online networks have different moral norms? How are the ethics of international affairs affected by virtual environments and behaviour? Do our laws and norms on violence apply equally to cyberspace? What is the role of collective morality in an international system dominated by the individual? Does increased power to the individual necessarily mean greater global justice, or is this prospect countered by new forms of injustice? Is a disordered world less just than a world with collective organization?

Knowledge production: Academic researchers, the media, policy-makers, and the public now engage with one another in new spaces—spaces that cannot be properly captured or understood through traditional research methods. How does the actual production of research need to evolve to leverage the network ecosystem? Can we evaluate how digital tools can help in the accumulation and distillation of knowledge in social sciences that rely on a traditional research paradigm? Can we employ digital tools to creatively expand the academic conversation, allowing collaboration between parties that, without the appropriate technology, have been unable to cooperate in the creation of knowledge? Do digital tools deliver a different type of knowledge than "analogue" tools?

International relations: How does the addition of digital information networks change some of the core questions and assumptions of international relations? In an international system in which the individual is the main unit, what is power and how is it exercised? What are the implications for levels of analysis in international relations? Are assumptions of anarchy more founded? What are the prospects for international cooperation? Does the rise of the individual dampen the impact of economics on international politics?

Technology: As much as possible, research needs to keep up with the incredibly rapid pace of technological change. The study of the impact of information technology on international affairs is particularly connected to this evolution. While the military is currently

developing swarm drones, for example, the academic community is still only beginning to understand the impact of the Internet on international systems. The radically differing pace of research advances versus technological development presents a real challenge to scholars. Part of the solution must be for some academics in all disciplines to be keenly attuned to boundary-pushing technology.

For the past 50 years, Canada has attained international status beyond its natural endowment in part through its successful use of state-based international organizations to promote individual rights and freedoms. In the evolving international architecture, such organizations are no longer the best vehicles for achieving such goals. For Canada to maintain its international reputation as a country that promotes the individual, it must devise a strategy that sees itself as a complement—rather than an obstacle—to the central networked actors of today's world. This means better understanding, engaging with, and embracing the actors, tools, and challenges of the networked world.

Bibliography

Albert, Réka, Hawoong Jeong and Albert-László Barabási (2000), "Error and attack tolerance of complex networks," *Nature*, vol. 406 (June), 378-382.

Ammori, Martin (2005), "Shadow government: Private regulation, free speech, and lessons from the Sinclair blogstorm," *Michigian Telecommunications and Technology Law Review*, vol. 12, 1.

Applin, Sally and Michael Fischer (2011), *A Cultural Perspective on Mixed, Dual and Blended Reality*, IUI Workshop on Location Awareness for Mixed and Dual Reality, LAMDa'11. Palo Alto, California, 13 February. Available at http://www.dfki.de/LAMDa/accepted/ACulturalPerspective.pdf

Axworthy, Lloyd (2000), "Axworthy Launches International Commission on Intervention and State Sovereignty," Address to the UN General Assembly, September 7.

Axworthy, Lloyd (1999a), "Address to the 54th Session of the UN General Assembly," *United Nations,* September 23.

Axworthy, Lloyd (1999b), "Address to the Standing Committee on National Defence and Veterans Affairs," March 31.

Axworthy, Lloyd (1998), "Diplomatic Conference Begins Four Days of General Statements," *United Nations*, June 15.

Balkin, Jack (1998), *Cultural Software: A Theory of Ideology.* New Haven, CT: Yale University Press.

Benkler, Yochai (2012), "Hacks of Valor: Why Anonymous Is Not a Threat to National Security," *Foreign Affairs* (April). Available at http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of-valor

Benkler, Yochai (2002), "Penguin, or, Linux and the Nature of the Firm," *Yale Law Journal*, vol. 112.

Boyd, Danah (2008), "Why youth (heart) social network sites: The role of networked publics in teenage social life," in D. Buckingham (ed.), *Youth, Identity and Digital Media*. Cambridge, MA: MIT Press.

Burkeman, Oliver (2012), "Inside Washington's high risk mission to beat web censors," *The Guardian,* April 15. Available at http://www.guardian.co.uk/technology/2012/apr/15/commotion-wireless-new-america-foundation

Castells, Manuel (2000), "Information Technology and Global Capitalism," in Will Hutton and Anthony Giddens (eds.), *On the Edge: Living with Global Capitalism*. London: Jonathan Cape.

Considine, Mark (2005), "Partnerships and Collaborative Advantage: Some Reflections on New Forms of Network Governance," *The Centre for Public Policy* (December).

Copeland, Daryl (2001), "The New Axworthy Years: Canadian Foreign Policy in the Era of Diminished Capacity," *Canada Among Nations*.

Davis, Jeff (2012), "John Baird points finger at gay rights abuses in African, Caribbean countries," *The National Post*, January 23. Available at http://news.nationalpost.com/2012/01/23/john-baird-points-finger-at-gay-rights-abuses-in-african-caribbean-countries/

Deibert, Ron (2011), "Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma," *The Citizen Lab*. Available at http://citizenlab.org/2011/11/behind-blue-coat/

Documents on Canadian External Relations (1949), vol. 15, chapter IV, "Ambassador in United States to Secretary of State for External Affairs," 492.

Ellickson, Robert (1991), *Order Without Law: How Neighbors Settle Disputes*. Cambridge, MA: Harvard University Press.

Fieschi, Catherine (2012), Personal Communication, February 22.
Froomkin, Michael (1997), "Internet as a Source of Regulatory Arbitrage," in Brian Kahin and Charles Nesson (eds.), *Borders in Cyberspace*. Cambridge, MA: MIT Press.
Gentzkow, Matthew and Jesse Shapiro (2006), "Media Bias and Reputation," *Journal of Political Economy*, vol. 114, 2.
Godin, Seth (2001), *Unleashing the Ideavirus*. New York: Hyperion.
Gross, Michael Joseph (2012), "World War 3.0," *Vanity Fair* (May). Available at: http://www.vanityfair.com/culture/2012/05/internet-regulation-war-sopa-pipa-defcon-hacking
Hargittai, Eszter (2007), "Whose Space? Differences among users and non-users of social network sites," *Journal of Computer-Mediated Communication*, vol. 13, 1.
Harper, Stephen (2011a), "Statement by the Prime Minister of Canada at an emergency meeting on Libya," March 19. Available at http://www.pm.gc.ca/eng/media.asp?category=3&featureId=6&pageId=49&id=4052
Harper, Stephen (2011b), "Statement by the Prime Minister of Canada on recent developments in Libya," February 21. Available at http://www.pm.gc.ca/eng/media.asp?id=4052
Haythornthwaite, Caroline (2005), "Social networks and Internet connectivity effects," *Information, Communication and Society*, vol. 8, no. 2, 125-147.
Horwitz, Sari, Shyamantha Asokan, and Julie Tate (2012), "Trade in surveillance technology raises worries," *The Washington Post*, December 1. Available at http://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAFFZOGO_print.html
Kuran, Timar (1995), *Private Truths, Public Lies: The Social Consequences of Preference Falsification.* Cambridge, MA: Harvard University Press.
Latour, Bruno (1997), "Train of thought: Piaget, Formalism and the Fifth Dimension," *Common Knowledge*, vol. 6, 170-191.
Lehrer, Jonah (2012), "Groupthink," *The New Yorker*, January 30.
Lessig, Larry (1998), "The New Chicago School," *Journal of Legal Studies*, vol. 27.
Morozov, Evgeny (2011), *The Net Delusion: The Dark Side of Internet Freedom*. Philadelphia: Public Affairs.

Pearson, Lester (1970), "On Human Survival," *Saturday Review*, June 13.
Rheingold, Howard (2002), *Smart Mobs: The Next Social Revolution*. New York: Basic Books.
Sengupta, Somni (2012), "The Soul of the New Hacktivist," *The New York Times*, March 17.
Shirky, Clay (2010), "The Shock of Inclusion," *The Edge World Question*.
Shirky, Clay (2008), *Here Comes Everybody: The Power of Organizing Without Organizations*. New York: Penguin Press.
Sundén, J. (2003), *Material Virtualities*. New York: Peter Lang.
Torrentfreak (2012), *ODDNS: Decentralized and Open DNS to Defeat Censorship* (April 7). Available at http://torrentfreak.com/oddns-decentralized-and-open-dns-to-defeat-censorship-120407/
Wendt, Alexander (1992), "Anarchy Is What States Make of It," *International Organization*, vol. 46, no. 2.