TOWARDS STEWARDSHIP IN CYBERSPACE

RON DEIBERT

Citizen Lab and Canada Centre for Global Security Studies,
Munk School of Global Affairs, University of Toronto

MARCH, 2012

CYBERDIALOGUE2012

WHAT IS STEWARDSHIP IN CYBERSPACE?

Canada Centre for
Global Security Studies

MUNK
SCHOOL
OF
GLOBAL
AFFAIRS

UNIVERSITY OF
TORONTO

The whole human memory can be, and probably in a short time will be, made accessible to every individual … It need not be concentrated in any one single place. It need not be vulnerable as a human head or a human heart is vulnerable. It can be reproduced exactly and fully, in Peru, China, Iceland, Central Africa, or wherever else seems to afford an insurance against danger and interruption. It can have at once, the concentration of a craniate animal and the diffused vitality of an amoeba.

— H.G. Wells, "World Brain: The Idea of a Permanent Encyclopedia" (1937)

The world's 7 billion people now share a single complex information and communications system, widely referred to as cyberspace.[1] Cyberspace functions, and arguably functions very well, despite no grand blueprint or central point of control. Born as an experimental research network in universities, what used to be the 'Internet' has mushroomed, more by accident than design, to become the information and communications operating system for planet Earth. A mixed common-pool resource that cuts across political jurisdictions and the public and private sectors, cyberspace has become, as Marshall McLuhan foresaw, 'our central nervous system in a global embrace.'

This unprecedented planetary-wide network produces a remarkable stream of innovations and social goods. Deep wells of knowledge, translated into multiple languages, are now instantly accessible to nearly everyone across the planet; H.G. Wells's fantastic notion of a world encyclopedia, written less than 80 years ago, is now no longer science fiction. Precise geo-locational coordinates down to the level of centimetres are now available in the palm of anyone's hand to manage scarce resources. Instantaneous information sharing—'crowd-sourced' among connected individuals—holds out the potential of revolutionising everything from election monitoring to disaster relief to disease outbreak predictions.

Yet as wonderful as the fruits of cyberspace are, the poisons are equally troubling. Malicious software that pries open and exposes insecure computing systems is developing at a rate beyond the capacities of security researchers to count, let alone mitigate. Massive data breaches of governments, private sector actors, non-governmental organisations (NGOs) and individuals are now seemingly a daily occurrence. Systems that control critical infrastructure—electrical grids, nuclear power plants, water treatment facilities—have been demonstrably compromised and targeted by state actors, risking a potentially catastrophic loss of life should anyone with malicious intent seek to cause widespread harm.

[1] The US Department of Defense presently defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (see US Department of Defense (2010) *Department of Defense Dictionary of Military and Associated Terms*. Joint Publication (JP) 1-02. Washington, DC: US Joint Chiefs of Staff, 86). This definition acknowledges that cyberspace encompasses more than the Internet and is an interdependent network of technological infrastructure of which the Internet is one part. I further extend this definition to include the regulatory level (the norms, rules, laws, and principles that govern cyberspace), and the sphere of ideas through which videos, images, sounds and text are produced and circulated amongst users.

These unfortunate byproducts of an open, dynamic network are exacerbated by increasing assertions of state power. Insecurity, competition, and mounting pressures to deal with collective action problems are together driving growing government interventions in cyberspace. Internet censorship at the national level, once thought to be impossible, is now a global norm. The OpenNet Initiative estimates that as many as 960 million people live in jurisdictions that restrict access to an open Internet in some manner.[2] Dozens of countries have adopted explicit cyber security strategies, including the development of offensive cyber warfare capabilities – conventional or otherwise. Recent leaks that provided details on U.S. and Israeli computer network operations that sabotaged Iranian nuclear enrichment facilities took few by surprise, as many suspected their hands in the Stuxnet virus in the first place. What was surprising was the calculated admission itself, the first instance of a major power taking credit for an attack on a critical infrastructure through cyberspace. The reactions to this admission remain to be seen, but will unlikely follow the same sophisticated and methodically precise tactics. Many countries will seek comparative advantage from the cyber criminal underground instead, stirring a hornets' nest of hacktivism and espionage from which they derive short-term strategic intelligence and security benefits. Adding to this dangerous brew, a mushrooming commercial market for offensive cyber attack capabilities is sprouting to service an arms race in cyberspace that is only just beginning.

Faced with mounting problems, policy communities may be tempted by extreme solutions. Proposals being debated in liberal democratic countries to censor the Internet in response to copyright violations, to entrust secretive signals intelligence agencies with the mandate to secure cyberspace for all of society, to loosen or even eliminate judicial oversight around data sharing with law enforcement, or to delegate policing of the Internet to the private sector – are all illustrations of such risks. These policies are antithetical to the principles of liberal democratic government and to the system of checks and balances and public accountability upon which it rests. Furthermore, they legitimise the growing desire of autocratic and authoritarian regimes to subject cyberspace to territorialised controls, and the censorship and surveillance practices that go along with it.

Left unchecked, these trends portend the gradual disintegration of what is in the long-term interest of all citizens – an open and secure commons of information on a planetary scale. The articulation of an alternative vision of security, one that protects and preserves cyberspace as a dynamic and open ecosystem, is thus urgently required. At the heart of this vision will be the elaboration of the proper rights, roles and responsibilities for all actors who share cyberspace – a combination of ideal political structures and virtuous or ethical behaviour. This essay is primarily about the latter, and a particular notion of ethical behaviour in cyberspace inspired by the concept of stewardship.

[2] OpenNet Initiative. (2012). "Global Internet filtering in 2012 at a glance," http://opennet.net/blog/2012/04/global-internet-filtering-2012-glance

WHAT IS STEWARDSHIP?

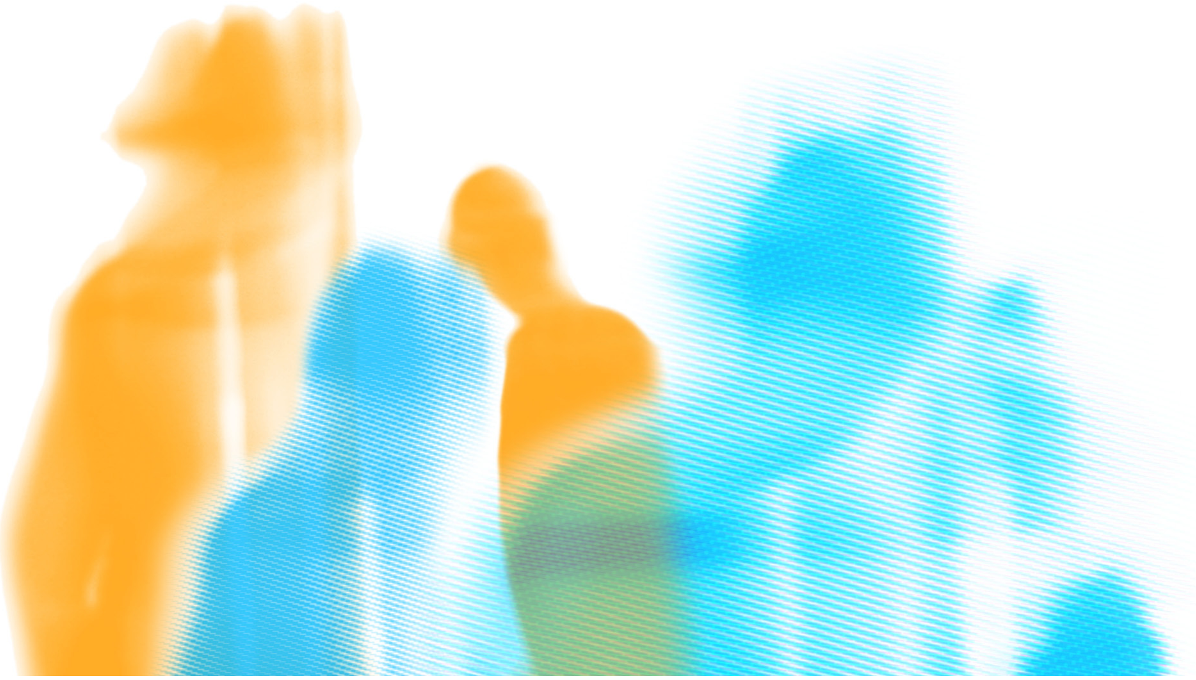
Stewardship is typically defined as an ethic of responsible behaviour in a situation of shared resources, typically with respect to the natural environment and the commons, such as the oceans and outer space. Cyberspace is not a pure commons as are these other domains. It is more like a mixed pooled resource, much of it in private sector hands, but with emergent shared properties that benefit all who contribute to it. Does stewardship have any relevance to such a domain? The first custodians of the Internet believed it did. Even if they did not use the language of stewardship self-consciously, the engineers and scientists who built and designed the Internet from the ground up saw their roles very much as custodians of some larger public good.

The concept of stewardship raises the bar when it comes to defining responsible behaviour: it goes beyond self-interest to demand an accountability of action in terms of both rights and responsibilities towards some larger shared social good. Stewardship implies a consideration of etiquette towards both others and the shared environment itself.

Stewardship is especially apropos because cyberspace is an artificial domain, one that requires constant tending. It is the first entirely artificial environment – without humans, it would not exist. This places us all in the position of joint custodianship of cyberspace. We can destroy it, or we can preserve and extend it. The responsibility is inter-generational, extending to those digital natives yet to assume positions of responsibility, but also linked to those in the past who imagined the possibilities for what something like cyberspace today presents. Imagine if H.G. Wells were here today to see how close we are to accomplishing his vision of a world encyclopedia, only to see it carved up by censorship, surveillance, and militarization?

Stewardship enriches what has become an almost empty euphemism: multi-stakeholderism. Governments, NGOs, armed forces, law enforcement and intelligence agencies, private sector companies, programmers, technologists and citizens all play a vital, unique and interdependent role as stewards of cyberspace – but for none is it an exclusive domain. Concentrating governance of cyberspace in a single global body, whether based at the United Nations or elsewhere, makes no sense from the perspective of stewardship in cyberspace. Stewardship in cyberspace implies numerous and distributed acts of governance at all points in the environment, from the local to the global, undertaken by a multiplicity of actors. Indeed, the only type of security that functions in an open, decentralised network is distributed security.

Stewardship happens constantly in cyberspace, even if the acts are not described in such terms. When Twitter unveiled a new national tweet removal policy, it felt obligated to justify its actions in terms of larger consequences, and the larger Internet community judged it according to principles of a kind very much like stewardship. As people entrust more and more data to third parties such as Twitter, how that information is handled, and with whom it is shared, must be based on more than mere self-interest and market considerations. Likewise, profiting from products and services that violate human rights, or exacerbate malicious acts in cyberspace, are unjustifiable in a context of common shared information and communication resources, regardless of how profitable such



products and services may be. Justifying them on the basis of compliance with local laws, as some companies have been known to do, is a hollow excuse in the framework of the higher standards that stewardship in cyberspace implies.

Stewardship can help moderate the dangerously escalating exercise of state power in cyberspace by defining limits and setting high thresholds of accountability and mutual restraint. The prevailing tendency for even liberal democratic governments to engage in mass surveillance without judicial oversight is fundamentally incongruous with stewardship in cyberspace. Governments have an obligation to set the playing field, ensure that malicious acts are not tolerated within their jurisdictions, and in doing so to set the highest possible standards of self-restraint through proper mechanisms of checks and balances. Privacy commissioners and other regulatory and competition oversight bodies are critical to stewardship in cyberspace as more and more information and responsibilities are delegated to private sector hands – equal to, if not more than, those agencies that deal with public and national security.

Since cyberspace is ultimately a network of individuals, stewardship extends also to each and every individual and to the networks of organisations that constitute what is broadly known as ‘global civil society.’ Breaches of computer systems and violations of privacy undertaken by vigilantes for whatever cause are unjustifiable and dangerous. Among those networks, universities have a special role to play as stewards of an open but secure commons of information since it is within the university system that the Internet was born and from which its guiding principles of peer review and transparency were founded. Protected by academic freedom, equipped with advanced research resources that span the social and natural sciences, and distributed across the planet, university-based research networks are the ultimate custodians and independent monitors of an open and secure commons and the codes, protocols and principles that surround it.

*****

We are at a crossroads in cyberspace. Mounting threats and an escalating arms race are compelling politicians to take urgent action. In the face of these concerns, those who care about liberal democracy on a global scale are in desperate need of a compelling counter-narrative to the reflex of state control. To be sure, stewardship is not a panacea. It will not immediately cease at once the raw exercise of power and competitive advantage in cyberspace. It will not bring malicious networks to their knees, or prevent cutthroat entrepreneurs from reaping a harvest from the market to exploit and degrade cyberspace. But it will help raise the bar, set the standards and challenge the players to justify their acts in more than self-interested terms. Above all else, it will focus collective attention on how best to sustain a common communications environment in an increasingly compressed political space.

Ron Deibert (PhD, University of British Columbia) is Professor of Political Science, and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto. He is a co-founder and a principal investigator of the OpenNet Initiative and Information Warfare Monitor projects. Deibert has been a consultant and advisor to governments, international organizations, and civil society/NGOs on issues relating to cyber security, cyber crime, online free expression, and access to information. He presently serves on the editorial board of the journals International Political Sociology, Security Dialogue, Explorations in Media Ecology, Review of Policy Research, and Astropolitics. Deibert is on the advisory boards of Privacy International, Access Now, and the Lake Ontario Waterkeepers.