

Towards stewardship in cyberspace

As the rewards and risks of the internet multiply, we need to ‘steward’ this information commons, much as we attempt to do for other shared resources

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

The world’s seven billion people now share a single complex information and communications system, widely referred to as cyberspace. 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 planet-wide network produces a remarkable stream of innovation and social goods. Deep wells of knowledge, translated into multiple languages, are now instantly accessible to almost everyone. Precise geolocational coordinates, down to the level of centimetres, are now available in the palm of anyone’s hand. Instantaneous information sharing – ‘crowd sourcing’ – holds the potential of revolutionising everything from election monitoring to disaster relief to disease outbreak predictions.

Threat to infrastructure

Yet, as wonderful as are the fruits of cyberspace, so are the poisons powerful. Malicious software that exposes insecure computing systems is developing at a rate beyond the capacities of security researchers. Massive data breaches of governments, private-sector actors, non-governmental organisations (NGOs) and individuals now occur daily. Systems that control critical infrastructure – electrical grids, nuclear power plants, water-treatment facilities – have been compromised, risking a potentially catastrophic loss of life

should anyone with malicious intent seek to cause widespread harm.

These unfortunate by-products of an open, dynamic network are exacerbated by increasing assertions of state power. Insecurity, competition and mounting pressures to deal with collective action problems drive growing government interventions in cyberspace. Internet censorship at the national level, once thought impossible, is now a global norm. The OpenNet Initiative estimates that 960 million people live in jurisdictions that restrict access to an open internet in some manner. Dozens of countries have adopted explicit cyber-security strategies, including the development of offensive cyber-warfare capabilities. Some countries actually benefit from the cultivation of the cyber-criminal underground, stirring a hornets’ nest of ‘hacktivism’ and espionage from which they derive short-term strategic intelligence and security benefits. A huge commercial market for offensive cyber-attack capabilities is sprouting to service the arms race that is only just beginning.

Extreme solutions may find resonance in the policy community. Proposals to censor the internet in response to copyright violations, to entrust secretive signals to intelligence agencies with the mandate to secure cyberspace for all, to loosen or even eliminate judicial oversight of data-sharing with law enforcement, or to delegate policing of the internet to the private sector – 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 control, and to the censorship and surveillance that go along with such control.

These trends portend the gradual disintegration of an open and secure commons of information on a global 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 its heart will be the elaboration of the proper rights, roles and responsibilities for all actors who share cyberspace.

Stewardship is typically defined as an ethic of responsible behaviour in a situation of shared resources, with respect to the natural environment and the commons, such as the oceans and outer space. Yet cyberspace is not a pure commons like these other domains. It is a mixed, pooled resource, much of it in private-sector hands, but with shared properties that benefit all who contribute to it. However, the concept of stewardship offers powerful guidance. In fact, stewardship is a natural fit for cyberspace governance, having been used explicitly by the engineers and scientists who built and designed the internet itself.

Stewardship goes beyond self-interest to demand accountability, in terms of rights and responsibilities to some larger shared social good. It is especially appropriate because cyberspace is an artificial domain 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 responsibility, but also linked to those in the past who imagined the possibilities for what something like cyberspace today presents.

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 an 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 cyberspace. Stewardship in cyberspace implies numerous and distributed acts of

governance at all points of 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 all the time in cyberspace, even if the acts are not described in such terms. When Twitter unveiled a new national tweet removal policy, it justified its actions in terms of larger consequences, and was judged according to principles of 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 is unjustifiable in a context of common shared information and communication resources, regardless of profitability. Justifying it on the basis of compliance with local laws is a hollow excuse, in the framework of the higher standards that stewardship in cyberspace imposes.

Limiting state power

Stewardship can help to moderate the dangerously escalating exercise of state power in cyberspace, by defining limits and setting thresholds of accountability. Today's tendency towards mass surveillance without judicial oversight is incongruous with stewardship in cyberspace. Governments are obliged to ensure that malicious acts are not tolerated within their jurisdictions, and to set the highest possible standards of self-restraint through proper mechanisms of checks and balances. Privacy commissioners and competition and other oversight bodies are critical 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 individual and to the networks of organisations that constitute global civil society. 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.

To be sure, stewardship is not a panacea. It will not immediately cease the raw exercise of power and competitive advantage in cyberspace. It will not destroy malicious networks or prevent cut-throat entrepreneurs from profiting from the market to undermine cyberspace. But it will help to raise the bar, set 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 to sustain a common communications environment in an increasingly compressed political space. ■

Governments are increasingly keeping an eye on online activity. Internet censorship at a national level, once thought impossible, is widespread

