STEWARDSHIP, SECURITY, and CYBERSPACE

JAMES A. LEWIS

Center for Strategic and International Studies
Washington, DC

MARCH, 2012

CYBERDIALOGUE2012

WHAT IS STEWARDSHIP IN CYBERSPACE?

Canada Centre for Global Security Studies

MUNK SCHOOL OF GLOBAL AFFAIRS

UNIVERSITY OF TORONTO

Who are the stewards of the Internet? Are they the grey-bearded men and women of technical organizations like Internet Engineering Task Force (IETF)? Are they drawn from civil society organizations concerned with cyberspace, or the ranks of business executives from the companies that provide related goods and services? Government agencies responsible for Internet activities might call themselves stewards, as could multinational entities like Internet Corporation for Assigned Names and Numbers (ICANN) or the International Telecommunications Union (ITU).

We can begin to define the concept of stewardship by putting it in the context of community, legitimacy, and governance. A steward is more than a stakeholder, and is responsible for some larger good. Responsibility (or stewardship) can be assigned or it can be assumed—it need not be recognized. Stewardship is linked to action. A steward who does not act to promote the larger good is not really a steward. Stewardship is not tied to ownership in that the steward need not own what he or she manages or protects. Stewards act on behalf of someone else, an owner or a larger community from whom their authority derives.

The concept of stewardship is most compelling when we think of the communities that are responsible for many of the Internet's technical management issues. The IETF is an archetype for this kind of self-organizing community. It is flat— without hierarchy or complex structure—and influence comes from expertise rather than position. It is famous for its emphasis on rough consensus and running code. Participants in IETF processes are the stewards of connectivity, whose success has shaped thinking about how the Internet should be governed. As the Internet has grown in size and importance, however, the IETF community model lacks the authority and expertise to scale into important international issue areas such as security and trade.

The communities that lay claim to cyber stewardship assert a degree of authority, but their goals as stewards differ in key areas. For example, what best serves commercial interests may compromise privacy and security. What best serves national security could compromise civil liberties. Civil society organizations may focus on a single issue at the expense of the larger public interest. The processes for mediating these disputes are weak. This may be only a transitional phase as cyberspace moves to new governance structures that resemble other international governance structures. Since these structures involve relations between sovereign states, who can be reluctant to acknowledge a higher authority, dispute resolution can also be limited, but there are formal processes and precedents for making binding decisions and resolving disputes.

The lack of a formal governance process means that those who assert stewardship are, in a sense, self-appointed. This has serious implications for their authority and legitimacy, others' acceptance of the steward's authority to take action, and is a severe and damaging limitation. Legitimacy is derived from the consent of the governed when they acknowledge authority and assent to its rules. Consent can be obtained either through coercion and force – the governed do not oppose the rulers out of fear – or through some participatory mechanism to indicate assent. The Internet has neither.

There are multiple sources of authority on the Internet. The most powerful include technical knowledge, ownership of the infrastructure (including software), and the ability to mobilize an amorphous community of users to act for some common goal. Governmental authority has been largely indirect— the influence of national laws and agencies on the technical, business, and civil actors who interact in cyberspace. This is beginning to change as governments assert a more direct role not only over their own national networks, but also over the larger transnational construct known as cyberspace. A community where force and consent are insufficient to provide authority will be unstable, provoking action from governments.

Moral authority or expertise can also provide influence, but moral authority is most effective when reinforced or "operationalized" by formal institutions. The lack of legitimacy makes the existing structure vulnerable to challenge. If we were to use the only existing democratic and representative body existing today, the UN General Assembly, and if we were to put to a vote the question of how the Internet should be governed and who should be its stewards, there would be rapid and dramatic change.

Stewardship is being redefined by the growing tension between the informal stewards of the Internet community and the official stewards appointed by governments. Some of the tension we see between the traditional Internet "stewards" and governments in arenas like the ITU and the General Assembly or in the debate over the future of ICANN comes from governments challenging and displacing the informal and unrepresentative governance processes that Internet stewards have been using for years. This displacement is a gradual extension of control through various mechanisms – law, regulations and courts. Governments are extending their control because they regard the current stewardship of the Internet as inadequate to meet the public interest, or in some cases, as a source of risk.

We can use several metrics to assess the Internet's stewardship. The stewards of the Internet have been very successful at promoting access and connectivity. They have created something that has never existed before – a globe-spanning network that instantaneously connects all individuals and devices that are part of it. The immense success of creating a framework that allows a multitude of divergent technologies to connect almost seamlessly is another triumph. If our metric is connectivity and technical efficiency, we can say that cyberspace arguably functions very well, in spite of lacking a grand blueprint or central organizing structure.

Other metrics are less promising. As a source of information, a kind of digital Gresham's Law applies to the stock of knowledge.[1] The Internet is an unsorted communal heap that has grown by accumulation and contains both trash and treasure. This has political implications at both the global and national level. One could say that the Internet as an informational device is a massive recreation of the work of the French encyclopedistes, philosophers, and scientists who worked jointly to create a massive database— a "systematic Dictionary of the Sciences, Arts and Crafts."[2] But the philosophers' notion of *systematic* was epistemological, involving a judgment about validity. For the stewards of the Internet, systematic means technical: the only judgment involves engineering feasibility and technical fidelity.

The comparison here might be with the

1 Which we can restate as "Bad ideas drive out good."

2 An online version of the The "Encyclopédie ou Dictionnaire raisonné des sciences, des arts et des métiers, par une Société de Gens de letters" can be found at http://encyclopedie.uchicago.edu/

stewards of a large research library who ensure that information comes with a date, that there is some reliability regarding source, and that fiction is clearly classified as such. The previous stewards of information—researchers, archivists, publishers— imposed a certain discipline. Perhaps this curtailed freedom of expression, but in exchange, it provided a higher degree of trust. The wisdom of the crowd is not an adequate substitute for the judgment of experts in such cases—when these expert judgments are not arbitrary dictates, but the result of reasoned debate subject to review and amendment.

Why this situation is a problem may not be readily apparent unless we consider the origins of computing. The pioneers of computing saw these devices as augmenting the human intellect, as a "collective memory machine," and as devices that would reduce the need for human intermediation in tasks. The uneven and unreliable nature of data on the Internet increases the need for intermediation; a human must step back and make a decision on validity. The requirement for human intermediation is one reason people complain of the flood of information they find difficult to process – the Internet as currently configured has reached its limits in the task of automating knowledge.[3]

These issues raise fundamental questions. Is the Internet the ultimate expression of democratic goals, where reason and knowledge will reform society? Or does information on the Internet erode consensus on the norms and values that guide individual action without providing an adequate process for rebuilding agreement?

3 Examples include the work of Douglas Englebert to develop a "tool for thought," and Vannevar Bush's 1945 essay "As We May Think." A longer discussion of these concepts can be found, as an introduction, in Thierry Bardini and Michael Friedewald, "Chronicle of the Death of a Laboratory: Douglas Engelbart and the Failure of the Knowledge Workshop," History of Technology, 2002

The political effect of a greater ability to communicate is unclear and, in the near term, not entirely positive. In the world of social media, there is a clear impetus for greater participation in political debate and decision-making, but this momentum is accompanied by an increased impulse for extremism and mistrust. These political effects – greater participation, reinforcement of extreme views - may follow a trajectory similar to the advent of the printing press, where the greater access to information it provided created powerful political forces that reshaped the relationship between government and citizen, but this process of necessary political adjustment may lie outside the scope of existing Internet stewardship.

The greatest and most pressing failure of Internet stewardship involves security. The legitimacy of the technical community that has played the most active stewardship role is undercut by its inability to secure the network. By reducing government responsibility, the inadvertent result of the multistakeholder approach has been to free governments from their normal international obligations. The porous technologies of the Internet and its global connectivity create a temptation that malicious actors are unable to resist. The traditional "stewards" lack both authority and the skill to intervene against malicious actors in cyberspace. If stewards cannot protect the resources entrusted to them or the people who use them, they have failed in their primary task.

The inability to adequately secure cyberspace will unavoidably drive change in governance and stewardship because it is one area where both authoritarian and democratic governments can agree. Providing security is a basic function for any government. They are increasingly reluctant to accept informal stewardship to secure an essential global infrastructure that

their economies depend on but that is also the source of new and powerful threats. Serious discussion of the military use of cyberspace among governments takes place outside the existing Internet governance framework and without the direct participation of "stewards" who lack the relevant expertise.

The protection of civil liberties on the Internet is a third metric for stewardship, but the results are mixed and require judgment on causality. By maintaining a technical architecture that limits the ability to restrict content, there has been some success in preserving the Internet as a space where freedom of expression and access to information is unconstrained,[4] but this power is diminishing as new technologies extend the span of control in cyberspace. In democracies, these controlling technologies may be irrelevant, or limited to blocking commercial actions to protect business interests. Ultimately, the protection of civil liberties will depend less on technology and more on existing institutions, such as the courts, and the willingness of those who control the tools of force and coercion to submit to the judgment of judges and elected legislatures.

Multistakeholder and democratic are not the same. Internet governance bodies have sought to create global processes where multiple stakeholders can have a voice in decision-making. These processes face at least three dilemmas. First, they assert authority they have not won or been given – the most common complaint against ICANN is that a corporation charted by the Commerce Department and incorporated in California is not a legitimate international institution, and discussions in various UN fora often end in stalemates over non-binding principles.

The second is the selection process for representation in the various stakeholder forums, which are often not adequately representative of the populations for whom they speak. Finally, the restricted authority possessed by various consultative bodies like the Internet Governance Forum or the World Summit on the Information Society limits their ability to take meaningful action.

The multistakeholder model, by including a broader range of participants than would be the case if the Internet was purely a business activity or restricted solely to government participants, provides diversity and perhaps a "balance of power" among competing interests. This is a valuable attribute, but as powerful new actors (in the form of national governments) assert a greater role in shaping cyberspace, the multistakeholder model by itself may be too fragile and the communal stewards too weak to provide adequate stewardship.

The concept of stewardship will change as new participants gain a voice in shaping the global network. These nations have different attitudes to the relationship between government, business, and society. The growth of these alternative governance models fragments authority and limits stewardship. The diffusion of interest created by a global institution (which is what the network has become) and the introduction of new actors with different values and concerns changes the political context for stewardship and governance.

The stakeholder approach, in simple terms, is a model for corporations to use in deciding how to address the concerns of clients, suppliers, and other groups affected by the corporations' decisions and actions. Extending this model to the Internet creates areas of political ambiguity. For example, the stakeholder approach is inherently "top-down;" the bulk of Internet users

4 There is a clear and difficult "trade-off" between reducing the need for human intermediation in assessing the value of data and preserving the ability to contribute freely.

have no voice in governance debates (or no ability to select the voices that purport to speak for them). In applying the stakeholder model to the Internet, however, we have to substitute an increasingly amorphous community with increasingly diverse interests for the corporation. Unlike a corporation, which owns its assets and is responsible to some legal authority for its actions, Internet ownership and responsibility are broadly distributed. Technical coordination by standards and protocols are at the core of the Internet. The Internet's core governance bodies have been those that set such standards and protocols, but they are of limited utility when it comes to problems of international security.[5]

Each nation carefully guards its authority over these international issues and surrenders its sovereign rights only in carefully defined circumstances or when compelled by superior force. Political decisions about whether an action complies with generally accepted international norms or whether the national interest outweighs adherence also shape national behavior. And while these decisions can be influenced by external pressure they are also jealously guarded. Governments are, in effect, the "stewards" of their national interests. As more nations become concerned with cyberspace, and as it grows in importance for the health of nations, governmental stewards will seek to expand their role at the expense of the informal community.

Stewardship and cyberspace are at a turning point. Political leaders and influential audiences perceive the cyber environment as unstable and insecure. Many nations see the risk of cyber war or cyber conflict as reaching an unacceptable level. National leaders believe their responsibility for security and stability means they must play a larger role in cyberspace. New "entrants" from the developing world regard existing forms of Internet governance as inadequate and unrepresentative. Increasing pressure on the current system comes from the belief that the current Internet governance structure is part of some larger strategy by the US to advance its interests. Government actions, the most obvious of which are the "Great Firewall" in China or Russia's SORM-2, have shown that cyberspace is not a commons, but instead a technical fabric that is owned, subject to national law, and manipulable by national policies. The political context for stewardship and governance has changed in ways that old models cannot control. Stewardship will change, but in ways we have not yet defined or even envisioned.

James Andrew Lewis is a senior fellow and Program Director at the Center for Strategic and International Studies, where he writes on technology, security and the international economy. Lewis received a Ph.D. from the University of Chicago; his current research involves the political effect of the Internet, asymmetric warfare, strategic competition, and technological innovation.

5 It is useful to consider the preservation of economic opportunity for a nation as part of its broader security interests.