Obama's Web 2.0 presidency

BY RONALD J. DEIBERT

Ron Deibert is the director of the Citizen Lab at the Munk Centre for International Studies, University of Toronto.

Barack Obama's successful election campaign has been proclaimed as momentous for many reasons, not least of which is the exploitation of digital media. Although previous campaigns have made use of the Internet and cellphones, Obama's innovation was to combine them with Web 2.0 technologies, like Facebook and Twitter, to mobilize vast communities of local volunteers and micro-fundraisers around a common cause.

A DEVOLUTION OF POWER?

Digital media—which include the global Internet, cellphones, and consumer electronic devices—infiltrate and give shape to every aspect of society, economics, and politics today. They are small, portable, and increasingly mobile. There are roughly 3.2 billion mobile phones in the world, with the highest growth rates occurring in the developing world. They are also global, not only carried through the vectors of business, social, and military networks, but also percolating from below through spontaneous grassroots development and individual ingenuity.

For years, theorists have grappled with the social and political consequences of digital media. Are they flattening power structures? Are they bringing about the end of sovereignty? Are they empowering individuals? Does the Obama campaign, and other innovative uses of social networking like it, represent a radical new devolution of power? The thesis put forth here is much less linear and tidy. The consequences for world politics of digital media penetration are mixed, chaotic, often contradictory, and therefore turbulent.

THE GEOPOLITICS OF CYBERSPACE—STATES STILL MATTER

It was once widely believed that states are too rigid, hierarchical, and cumbersome to control flows of digital media.

> Digital media—which include the global Internet, cellphones, and consumer electronic devices— infiltrate and give shape to every aspect of society, economics, and politics today.

That assumption has not been shared by many states themselves, especially in recent years. After 9/11, the methods and tools of "hard politics" entered into the soft power realm of digital media. The digital media environment emerged as a battlefield, fought within and across each of its spheres, from physical infrastructure, to code, to the cognitive realm of ideas. Dozens of states routinely block access to information deemed strategically, culturally, or political threatening, and these blockages are often timed to coincide with key political events, such as elections. The methods employed range from filtering software installed at key Internet chokepoints and gateways, to computer network attacks, to the strategic propagation of malware and disinformation through open channels.

Often operating deep within the subterranean infrastructure of the Net, without transparency and accountability, these methods have as their ultimate aim the shaping of the ideasphere, a borderless and amorphous realm. The ancient art of propaganda has morphed from a strategic appendage to the centrepiece of 21st-century military strategy. Ideas are the object of geopolitical contestation, as much as natural resources and territory have been in the past, with much greater attention paid to techniques of persuasion, psychological operations, and viral marketing for military strategic ends. Because the geopolitics of digital media are inherently transnational, states' information-warfare activities are themselves internationalized, and thus (ironically) are contributing to the unbundling of the sovereignty paradigm.

DISTRIBUTED INGENUITY—CAN BE MALICIOUS TOO

State acts of cyber warfare described above are highly chaotic, volatile, and inherently unpredictable, in part because of the distributed nature of the digital media environment itself. It is well known that the Internet exhibits great complexity; its structure effectively empowers users at end points or edges of the networks. Given the seamlessly linked character of these networks, innovation at these edge locations can have system-wide effects. The system as a whole is thus dynamic and occasionally turbulent. Although states may seed cyber warfare campaigns, the campaigns have a tendency to take on a life of their own because of the unavoidable participation of multiple actors swarming from edge locations, as evidenced in Estonia, Georgia, Tibet, Burma, Pakistan, and elsewhere.

The most recent conflict between Hamas and Israel offers a case in point. The Israeli Defense Forces' campaign has been highly influenced by the lessons learned from the 2006 war with Hezbollah, particularly the need to ensure that the public relations part of the battle—control of the ideasphere— was not lost. Telecommunication networks and cellular towers were targeted as part of the IDF incursion into Gaza, and foreign journalists cordoned off to limit outside access. Such methods can-

not prevent distributed acts of swarming, however, on both sides of the conflict. For example, members of a Moroccan-based hacking group called "TEAM-Evil" infiltrated the database of the official Israeli domain registrar, DomaintheNet. This gave them the ability to alter the name servers of several important Israeli websites, including the popular Israeli online news service, YnetNews.com, redirecting its traffic to a page containing pro-Hamas information.

Tens of thousands of Israeli websites were defaced by individuals and groups based in Turkey, Lebanon, and Iran, among others. On the other side of the conflict, a group of Israeli computer science students created a website advertising a downloadable Trojan horse that allows users all over the world to "turn over" their PCs to control servers that in turn employ them to execute distributed denial-of-service attacks on Hamas-related websites. Their website claimed that several thousand users signed up. However much the parties to a conflict try to manage the idea-zone to suit their strategic aims, swarms of groups and individuals intervene, leading to unpredictable and potentially highly chaotic outcomes.

FLATTENED, FUSED, AND MONITORED

The distributed ingenuity described above has led many to believe that one clear consequence of digital media is the empowerment of individuals and grassroots organizations at the expense of more hierarchical centres of power, such as states and corporations—a kind of "flattening" of power, to borrow a phrase popularized by the journalist Thomas Friedman. Flattened power is derived, in part, from the platforms of Web 2.0 and 3.0, including ubiquitous, distributed, and sharable computing systems and databases, social networking platforms, three-dimensional shared spaces (for example, Second Life), open protocols, and "intelligent" applications that allow for machine learning and exploitation of the semantic web. The thesis is dramatically illustrated by numerous examples

> **The domain of digital media is being militarized and mined at the same time as it is exploding with ingenuity and grassroots empowerment.**

of grassroots advocacy campaigns, new electoral strategies, and coordinated mass mobilizations, including Obama's dramatic election victory referred to above.

However, the flattened power thesis needs to be qualified in several important ways. First, many of the Web 3.0 platforms are serviced by third-party private intermediaries on so-called cloud computing systems in an oligopolistic market dominated by a few large Internet service companies, like Google, Yahoo, and Microsoft. These companies sit on top of, and thus control, vast rivers of data, which they can then archive, fuse, recommercialize, and mine. Because many of their operations cross territorial boundaries and include jurisdictions that do not respect human rights or the rule of law, the consequences of the storage of this data can be profound and disempowering. For example, a recent report uncovered a massive surveillance system on the Chinese version of the popular networking phone system Skype, which was operated by the company in collusion with the Chinese government. Millions of encrypted chat messages and phone numbers and other personal

details were uploaded and stored onto insecure servers in China, to be shared with the Chinese public security bureau. Revelations such as these can create anxious and insecure publics who lack trust in digital media because of the lack of transparency and accountability. Self-censorship and political restraint can become the norm.

Second, and related, traditional centres of power, such as state intelligence agencies, are effectively exploiting the very same intelligent tools and distributed databases to monitor the activities of individuals. These efforts are enhanced by rapid advances in data mining, fusion, and visualization tools as well as the voluminous amount of personal information that is voluntarily supplied by the individuals using the social networking platforms. Today's job of mass surveillance is thus enhanced dramatically by the extent to which users willingly upload images, videos, and updates of their daily lives, all cross-referenced, geo-locationally fixed, and individually tagged, and thus ripe for picking by both public audiences and determined private actors.

THE GLOBAL VILLAGE— COMPRESSED

The domain of digital media is being militarized and mined at the same time as it is exploding with ingenuity and grassroots empowerment. This suggests a highly volatile mix of power politics, but one that operates in multiple jurisdictions simultaneously and involves both public and private actors, all at an extremely high rate of speed. While the Obama campaign and other innovative uses of digital media are remarkable, the geopolitical battles over and through digital media have not disappeared and power still matters. ❧