TheSecDevGroup

Preparatory Project

Open empowerment:
How digital natives are changing the world, and what it means for democracy, human rights, criminality and security

Time magazine called 2011 the year the protester. By its own admission, its person of the year could just as well have been *the network*. The year marked a coming-of-age of networked movements, and network power. It highlighted how a new digitally-empowered generation is using technology to amplify their political and economic muscle worldwide.

In 2011 *digital natives*[1] leveraged Cyberspace to organize and change their worlds:

- Across the Middle East and North Africa, technology savvy youth used social networking sites to organize and advertise political protests that toppled entrenched regimes through coordinated but largely leaderless resistance;

- In the United Kingdom, rioters used social networking sites and instant messaging to coordinate looting activities in the summer of 2011 outmaneuvering and overwhelming local policing;

- In Latin America, narco-traffickers used cyberspace to organize and manage an underground, global economic enterprise. At the same time, they used Facebook and other social media tools to deliver threats, extort money, and parade kidnap victims; Similar groups are doing likewise in areas of Western Africa and the Commonwealth of Independent States (CIS).

- Across the globe, cybercriminals, spies and warfighters incurred grave costs and security breaches for almost every national government. Cyber crime damage (alone) is estimated to cost the global economy some $ 1 trillion per year.

As this new generation of digital natives experiment with finding their political and economic *voice*, they are driving change on a global scale. Their actions and capacities reveal a bewildering array of opportunities and threats that cut across issues of democratic empowerment, human rights, criminality and security. In so doing, they present new challenges for all governing institutions, as the lines between legitimate and illegitimate, civil and uncivil action become blurred and redefined.

For many governments and regimes, the knee-jerk reaction to cyber-enabled 'threats' –- however defined -- has been to securitize cyberspace by imposing censorship, surveillance, and other forms of control. During the "Arab Spring' for example, Egyptian authorities invoked a near total shutdown of the internet. During the 2011 riots in the United Kingdom, the government considered extreme online controls, although these

[1] The term "digital natives" refers to those born in the era of digital technology, and who have interacted with it from an early age, resulting in their greater understanding of its workings and

were not enacted. Other states with strong traditions of state intervention into political and economic affairs – like members of the Shanghai Cooperation Organization (SCO) – are actively enacting strict domestic controls that seek to promulgate this model globally.

But as governments and regimes act to protect their citizens or their own stability, the openness of cyberspace -- meaning its property as a global, inter-operable network of networks that enables unrestricted communication – is under threat. This is a problem. Historically, cyberspace openness has been key to its capacities to enhance productivity, prosperity, communication, good government, personal and communal empowerment as well as innovation.

The challenge of finding an appropriate balance between cyberspace openness and security – that is, the future governing the cyber-commons -- is topping foreign policy agendas across the globe. But there are no easy answers.

Finding a way forward will require evidence-based research on how digital natives are using cyberspace, what effects state policies to securitize cyberspace are having (both intended and unintended), and where the holes are in existing governance architecture and thinking. It will also require creative thinking on how new forms of cyber-agency can strengthen democratic institutions and functioning, how cyberspace security can be achieved without eviscerating openness and what alternative policy options might look like.[2]

This concept note outlines a short-term preparatory research project aimed at developing a longer-term research endeavour around these questions. The longer-term objective is to create a global body of evidence-based research that documents the new political and economic agency of digital natives (be it for social change, community empowerment or personal gain) and the effects of on-going policy initiatives to securitize cyberspace. This research will feed broader thinking on policy options that find a balance between preserving cyberspace openness and ensuring security.

The proposed preparatory project will explore these issues with a specific geographical focus on Latin America, where the contest between securitization and preservation of openness in cyberspace is principally driven by threats to state authority posed by transnational criminal gangs and narco-trafficking. In general, Latin American governments are democratically elected, meaning that the politics of control is less of a factor driving securitization (or argument against openness) than in the Middle East and Asia. In addition this region is understudied with respect to documenting state efforts to control cyberspace.

The preparatory phase will be a joint effort between the SecDev Foundation and the Iagarpe Institute based out of Rio de Janerio.[3] Principal investigators have a strong mix

---

[2] Deibert, Ronald and Rafal Rohozinski. 2010. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy.* 21:4, 42-57.

[3] The Igarape Institute is an innovative social cooperation agency devoted to issues of security and development (see http://www.igarapesocial.com.br/home/index). Based out of Rio de Janeiro, it features a network of partners across Latin America and the Caribbean, North America and Western Europe. The organization undertakes research and policy development with public, private and non-

of experience looking at the evolution of controls in cyberspace and the changing ways in which non-state actors are leveraging cyberspace for economic, social and political change.

A. Background

Every day, news headlines document how the Internet is fundamentally transforming politics and security: from the Arab spring, to the Occupy movement, Anonymous, the Syrian Electronic Army, cybercrime, GhostNet spy rings and the beheadings of Mexican bloggers.

These reverberations are marked by an important demographic component. The vast majority of cyber-empowered users are under the age of 35. They are the first "networked generation." According to some figures, approximately 80% of those under 25 regularly use some sort of social media.

These changes are likely to have a significant impact in the developing world for several reasons:

- Most new internet users live in the developing world: Users in the Euro-Atlantic zone now constitute only 40% of the global share,[4] and that proportion continues to decline. Beyond this, three out of five global *netizens* are resident in fragile or failing states.

- Digital natives are using cyberspace to pursue concrete political change. In countries where democratic governance mechanisms are loosely rooted or largely absent, and where freedom of speech is problematic, digital natives are leveraging technology to express discontent, demand action, attract global sympathy and pursue collective direct action. Real world activities have gone online to great effect, as the Arab Spring showed the world.

- At the same time, criminal gangs and other para-state groups are leveraging Facebook, Google, Twitter, and other technologies for control, intimidation, and the pursuit of economic and political agendas. Developing countries are struggling to adapt to the challenges consequences of networked crime, politics,

governmental actors on issues of violence prevention and reduction, international peace support operations, and global drug policy. The Institute has undertaken work in partnership with the Organization for Economic Cooperation and Development's Development Assistance Committee (OECD-DAC), the United Nations Development Program (UNDP), the United Nations Department of Peacekeeping Operations (DPKO), the Open Society Foundation (OSF), Itau, and a range of bilateral and multilateral partners including Canada, Norway and the United Kingdom.

[4] "World Stats." 2011. *Internet World Stats*. http://www.internetworldstats.com/stats.htm (accessed 24 November, 2011).

and militancy. Typically, states have attempted to establish authority in cyberspace through censorship, strict content controls, enhanced surveillance, and in some cases calls for the creation of national intranets. Control has been the dominant response to the new crisis of state authority.[5]

- However, government efforts to secure cyberspace may end up also de-legitimatizing and criminalizing civilian online protest and other forms of civil disobedience. Much thinking is needed on where the line between civil versus uncivil disobedience must now be drawn. For example, denial of service attacks -- a form of *hacktivism* practiced against online businesses or other institutions dependent on an online presence – are seen by some as criminal, full-stop. Others see them as equivalent to picket lines, which were used effectively by labor movements to put pressure on institutions in the industrial age.

These issues are intensely complex and contentious. This is true even for highly developed countries – where institutions are better adapted to adjust to changes in society through the systems of checks and balances. For developing countries with weaker institutions or stronger traditions of state control, the capacity to chart appropriate paths forward is exceedingly limited.[6]

It is critical to build knowledge and understanding of the emerging political and economic agencies of digital natives, and to consider how these will impact traditional political institutions and governance mechanisms.

B. Central research questions

Arguments for and against the preservation of cyberspace as an open domain generally focus on issues of privacy and transparency. But the issue of preserving openness may become more central as developing countries adapt to the burgeoning digital generation. Managing this transition by adapting institutions and establishing checks and balances is vital to ensure that democratic institutions remain in step with the social transformations brought about by technological change.

But adaptation will be a challenge, especially given the strong arguments in favor of securitization. The alleged threat to state legitimacy and the subversion of institutions by empowered criminal and militant actors make it difficult to argue for the preservation of openness and for greater tolerance of online forms of expression. Striking an appropriate balance is critical.

The central research questions to be explored in the preparatory phase, and anchored in short exploratory case-studies of selected Latin American contexts are:

---

[5] Deibert, Ronald Rohozinski, Rafal et al. 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. The MIT Press: Cambridge and London.

[6] Deibert, Ronald, Rohozinski, Rafal, et al. 2012.*Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. The MIT Press: Cambridge and London.

1) In what ways are digital natives leveraging cyberspace to pursue political, social or economic agendas that also impact on issues of state (or regime) security, citizen security and governance. What have been the effects on state-society relations?

2) How have affected governments reacted to these new forms of empowerment? What changes in cyber policy have been pursued and with what assumptions and what effects? What are the potential longer-term effects?