Area: Spain’s International Image and Public Opinion
ARI 144/2009
Date: 14/10/2009

Geopolitics 2.0 (ARI)

Matthew Fraser[*]

Theme: An entirely new form of virtual weaponry is transforming the dynamics of geopolitics.

Summary: The threat of cyber warfare is not new. The Internet was a product of the Cold War built in the 1960s by US military scientists to protect American communications infrastructure against a Soviet nuclear strike. Nearly a half century later, those threats remain. Today, however, cyber weapons are not only in hands of enemy and rogue states, but are being exploited by isolated individuals ranging from bored teenagers to wild-eyed terrorists. Today the impact of Web 2.0 goes beyond political mobilisation inside countries and digital diplomacy between states. It now includes virtual weaponry that has brought an entirely new form of warfare which is transforming the dynamics of geopolitics. We call this new global reality Geopolitics 2.0, which is –broadly speaking– characterised by *three* significant shifts: (1) states to individuals; (2) real-world to virtual mobilisation and power; and (3) old media to new media. Forced to react to the impact of these three Geopolitics 2.0 shifts, states are alternatively censoring or deploying Web platforms to achieve their goals and assert their influence –and in some cases, they are doing both–.

Analysis: In the aftermath of Iran’s massive street protests in June, no one was surprised when that country’s authoritarian regime blamed the unrest on Western intelligence agencies and big media organisations like the BBC and Voice of America. This time, however, the ruling mullahs’ litany of accusations included a new list of Western enemies: Twitter, Google, YouTube and Facebook.

Web 2.0 social networks had indeed played a powerful role during the uprising –not only in mobilising action inside Iran, but also in influencing global opinion–. The global media described the turbulent events in Iran as a ‘Twitter Revolution’ due to the widespread use of ‘tweets’ to organise spontaneous protests and disseminate information about what was happening in the country. Also, a young Iranian protestor called Nada became a tragic icon for the Iranian protest when, after being shot during a bloody repression, video images of her bleeding to death in the streets of Tehran were posted on YouTube, provoking horror and outrage throughout the world.

While the Iranian regime was not toppled in the summer of 2009, the ‘Twitter Revolution’ marked a turning point in global politics. Whereas in the past states were acutely conscious of the power of traditional media like CNN and the BBC in shaping world

[*] *Senior Fellow at INSEAD, Adjunct Professor at the American University of Paris and the Institut d’Etudes Politiques de Paris.*

opinion, the sudden explosion of Web 2.0 networks was imposing a new lexicon on the emerging geopolitical realities of digital diplomacy. The so-called ‘CNN Effect’ was now the ‘YouTube Effect’.

The powerful significance of this shift was not lost on Barack Obama as he moved into the White House in early 2009. In fact, President Obama owed his electoral victory in part to the mobilising power of Web 2.0 networks. As a candidate, Obama –constantly pictured thumbing his BlackBerry– had run a campaign that shrewdly leveraged not only Facebook, Twitter and YouTube, but also MySpace, Twitter, Flickr, Digg, BlackPlanet, LinkedIn and many other social networks. Obama’s masterful use of Web 2.0 platforms marked a major e-ruption in electoral politics –in America and elsewhere–. Since the US presidential elections of 2008, political campaigning has been shifting from the old system of top-down political machines towards Web-based mobilisation that gives a powerful role to the bottom-up dynamics of online social networks.

Obama also learned first-hand during the 2008 campaign how the Web can be used as an offensive weapon in political warfare. Hackers had broken into his election team’s computer system and stolen sensitive information about campaign travel plans and Obama policy positions. After being sworn in as President, Obama offered this reflection on that experience: ‘It was a powerful reminder, in this information age, one of your greatest strengths –in our case, our ability to communicate to a wide range of supporters through the Internet– could also be one of your greatest vulnerabilities’.

Not surprisingly, President Obama quickly grasped the strategic importance –and potential threat– of Web-based networks for America’s role as a global superpower. The US and other Western powers possessed reliable intelligence that numerous states –in particular Russia, China and North Korea– were engaged in cyber warfare in various forms: espionage, black propaganda, Web vandalism, data theft, cyber attacks on critical infrastructure and denial-of-service attacks. Facing these threats, one of the first measures President Obama announced after taking office was a White House programme to bolster America’s defences against cyber attacks. Declaring that cyber warfare was ‘one of the most serious economic and national security challenges’ facing America, President Obama earmarked US$335 million for securing US Internet infrastructure and appointed a White House ‘cyber czar’. The Pentagon meanwhile was spending more than US$100 million to repair and strengthen its computer networks. In the US Congress, four Senators were introducing a new bill called the *Cybersecurity Act*.

At the same time, the Pentagon signed off on the creation of a US ‘Cyber Command’, headed by Lt.-Gen. Keith Alexander, that was expected to be operational by late 2010. General Alexander declared that, in his new role, his mission was to ‘defend vital networks and project power in cyberspace’. While the Cyber Command’s work remains top secret, it is believed that its cyber-security efforts include blocking thousands of foreign electronic attacks on US network systems that occur every year.

‘Our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security’, noted Defense Secretary Robert Gates in an internal Pentagon memo. ‘To address this risk effectively and to secure freedom of action in cyberspace, the Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations’. Gates had good reason to be on high alert about a cyber threat. In 2008, Chinese military hackers were believed to have broken into an unclassified e-mail system in his own Pentagon office, creating embarrassment at the highest levels of the US government and triggering an immediate review of Pentagon IT procedures. And yet only a year later, Chinese and Russian cyber hackers were believed to have infiltrated the US electrical grid, leaving behind software programmes to disrupt the entire system.

The threat of cyber warfare is not new. In fact, the Internet itself –a product of the Cold War– was built in the 1960s by US military scientists to protect American communications infrastructure against a Soviet nuclear strike. Nearly a half century later, those threats remain. Today, however, cyber weapons are not only in hands of enemy and rogue states, but are being exploited by isolated individuals ranging from bored teenagers to wild-eyed terrorists. Today the impact of Web 2.0 goes beyond political mobilisation inside countries and digital diplomacy between states. It now includes virtual weaponry that has brought an entirely new form of warfare which is transforming the dynamics of geopolitics. We call this new global reality Geopolitics 2.0.

Geopolitics 2.0 is, broadly speaking, characterised by *three* significant shifts: (1) states to individuals; (2) real-world to virtual mobilisation and power; and (3) old media to new media.

States to Individuals

The first shift is from a state-centric approach in international relations towards a new dynamic involving a widely disparate number of non-state actors, even individuals, who can use Web platforms to exert influence, threaten states and inflict violence.

This shift has been occurring for some time, as states lose their monopoly as the exclusive actors on the global stage, but is now accelerating due to the impact of Web 2.0 networks. Geopolitics 2.0 does no evacuate state-to-state conflict. Make no mistake, states are using Web 2.0 instruments against other states. Communist North Korea is widely suspected, for example, of being at the origin of cyber attacks against neighbouring South Korea and other countries. Another example occurred in April 2007, when the normally tranquil nation of Estonia came under a cyber attack –targeting government, banks and media– following the relocation in that country of a Soviet war memorial. The Estonian government blamed the Kremlin for the sudden and unexpected cyber attack. While the Kremlin denied any direct involvement, the incident prompted the NATO military alliance to step up its readiness for cyber warfare.

What is unique about Geopolitics 2.0, however, is that Web networks like Google and YouTube empower not only states and non-state organisations, but also isolated individuals who can, due to low entry barriers, act upon global events –both constructively and destructively–. The Web 2.0 revolution has allowed individuals with virtually no resources to act and exert influence on the same playing field as powerful states that control massive economic and military resources. Today a lone hacker or influential blogger can play cyber David against Goliath states. This was powerfully demonstrated in 2009 when the Russian government allegedly inflicted a denial-of-service attack on Twitter in order to neutralise a single blogger in Georgia. Twitter users world-wide faced a paralysing brown-out because the Kremlin had launched a cyber attack against one individual.

The Georgian blogger turned out to be a 34-year-old economics professor in Tblisi who –known only as *Cyxymu*– had previously been unknown on the international stage. The identities of many individuals using Web 2.0 platforms in cyber war activities are, in like manner, either unknown or difficult to discover. This marks a major shift from previous models of geopolitics, where the main actors have been either states or other easily identifiable non-state actors, including terrorist groups like al-Qaeda. In Geopolitics 2.0, the identity of individual actors in the global system is frequently not apparent, and sometimes a baffling mystery. When hackers and cyberspies attack, governments may accuse China or Russia, but its origins and perpetrators are never verified with total certainty. In short, it's possible to be a significant actor in the global system, and inflict major damage on traditional states, without ever becoming known, let alone apprehended and punished.

Real-world to Virtual Mobilisation and Power

The second shift is from 'real-world' to 'virtual' forms of mobilisation, action and aggression.

The use of Twitter in Iran provided a powerful example of how Web 2.0 networks diffuse power to the periphery. In Iran, an authoritarian regime was so destabilised at first by the 'Twitter Revolution' that it was forced to physically repress its own population to prevent its own overthrow. In liberal democracies, Web 2.0 platforms like Facebook, YouTube and Twitter are now indispensible tools of electoral mobilisation and civic organisation. All governments are now acutely aware that their citizens can use these tools to voice their views, organise action and even challenge their authority.

In terms of coercive power, we are witnessing the same shift from the vertical centre to the horizontal periphery –or, expressed differently, from military 'hard power' to 'virtual power' forms of aggression in cyberspace–. Virtual power is different from 'soft power' in one important aspect: whereas the latter conveys values through culture, consumer behaviour and lifestyle (from Mickey Mouse to McDonald's), virtual power is located exclusively in cyberspace. America is a soft-power superpower, but is more vulnerable in the sphere of virtual power. This explains why the US is scrambling to invest massively in programmes that strengthen their arsenal of cyber weaponry –both offensively and defensively–. Lt.-Gen. William Shelton, the US Air Force's chief of warfighting integration, has said that in the past the Pentagon relied too heavily on industry efforts to respond to cyber threats. This industry-led approach, he added, failed to keep pace with the threat from cyber space.

'Threats in cyberspace move at the speed of light, and we are literally under attack every day as our networks are constantly probed and our adversaries seek to exploit vulnerabilities', General Shelton told the House Armed Services Committee in May 2009. A US National Security Council report concluded meanwhile that the American government's policies on waging cyber warfare have been ill-formed. While these statements may be motivated by a desire to obtain more substantial budget allocations, it cannot be doubted that they reveal how states –with their traditional institutional bias in favour of 'hard power'– have been slow to understand the velocity and significance of the cyber war threat.

Today, the so-called 'military-industrial complex' may need to rely less on giant arms manufacturers and four-star generals and more on computer geeks with formidable skills on videogames like *World of Warcraft*. That assertion may seem flippant, but it is actually a fact. The US Army is now using Web 2.0 platforms like Facebook and YouTube as recruitment tools and, what's more, is looking specifically for certain skills sets that include familiarity with virtual worlds and online videogames. The example is being set at the highest level of command: the US Joint Chiefs of Staff is on Twitter and has a Facebook 'fan' page. The British army, for its part, actively encourages its soldiers to use Twitter and Facebook. The CIA meanwhile has its own internal wiki, called Intellipedia, which is used as an information-sharing network that replaces old bureaucratic silos with a transparent collaboration system to gather intelligence on potential threats. As the new generation of so-called 'millennials' move into positions of responsibility in government and the military, they will bring with them powerful cyber skills that will be instrumentally useful in espionage and warfare.

Old Media to New Media
The third shift is from old media (like CNN, BBC and Al-Jazeera) to new media like Google, YouTube, Twitter and Facebook as effective platforms of global diplomacy, communication and opinion shaping.

In the past, governments have used mass media to wage information warfare. Prominent statesmen, including Presidents and Prime Ministers, have been willing to appear on CNN and the BBC to be interviewed about their positions and policies, and state and non-state actors have exploited the global media to stage events –and pull off stunts– to attract attention to their causes. Old media have been the privileged forum of global diplomacy. The era of old media dominance is coming to an end. We are witnessing a definite shift in favour of new media, not only with the emergence of Web-based forms of journalism, but more importantly through the explosion of platforms like YouTube, Google Facebook and Twitter as instruments of information and propaganda. Web 2.0 platforms are powerfully effective tools for mobilisation –or 'digital activism'–.

The Gaza crisis in 2008 provides an excellent example of shift towards new media. Shortly after Israel launched its military operation, a Jewish American citizen called Joel Leyden created a Facebook group called 'I Support the Israel Defense Forces in Preventing Terror Attacks from Gaza'. At the same time, an Arab called Hamzeh Abu-Abed created a Facebook group called 'Let's Collect 500,000 Signatures to Support the Palestinians in Gaza'. Intrigued by the leveraging of Web 2.0 networks on both sides of the crisis, *Time* magazine published a story under the headline 'Facebook users go to war over Gaza'. Most of these Facebook initiatives were the work of individuals. But states also joined the Web 2.0 propaganda campaign to get out their message. The Israeli Army, for example, launched its own YouTube video channel in an effort to win the global PR battle by uploading videos showing carefully pinpointed strikes against terrorist targets.

Forced to react to the impact of these three Geopolitics 2.0 shifts, states are alternatively censoring or deploying Web platforms to achieve their goals and assert their influence –and in some cases, they are doing both–.

Authoritarian states routinely imprison so-called 'cyber-dissidents'. In the Middle East, for example, Syria has jailed bloggers and blocks websites (including Facebook and YouTube) deemed a security threat. In Egypt, an Arab country that enjoys open diplomatic relations with the West, the government has punished online criticism of the state. Beyond the Middle East, the Chinese regime has imprisoned cyber-dissidents and shut down websites including YouTube, particularly over sensitive issues such as Tibet. Indonesia has banned both YouTube and MySpace. Other states that have banned websites or imprisoned cyber-dissidents include Iran, Saudi Arabia, Libya, Belarus, Burma, North Korea, Tunisia, Turkmenistan, Uzbekistan and Vietnam.

Liberal democracies, while undoubtedly developing their cyber war capabilities, are particularly focused on the potential danger of Web 2.0 forms of terrorism. It is believed that terrorists are using Web platforms like Google Earth to locate potential targets, especially in countries like Israel. This may explain why Google has pixilated sensitive zones in Israel and elsewhere in the world that could come under a terrorist attack. The findings of a 'Dark Web' research project at the University of Arizona tracked Jihadist extremist groups using Web 2.0 media. The study, published in 2008, came across an alarming number of Jihadist blogs, including one posting news updates about so-called 'occupied Islamic countries'. Jihadist bloggers were also active on YouTube, uploading videos featuring explosives, attacks, bombings and hostage-taking. On Second Life, meanwhile, a 'Terrorist of SL' attracted 228 members and another group called 'Liberation Front' counted 65 followers. The 'Dark Web' study concluded: 'Many of the Web 2.0 content providers may only act as Jihadist sympathisers or information dissemination agents for radical extremist materials. Most of them may not be the original content creators, i.e., the groups who performed the violent acts. However, their role and importance as online information dissemination agents or resource hubs cannot be underestimated'.

Some contend that Web 2.0 social networks can be anti-democratic even in liberal democracies. They warn against an ever-present danger that states will succumb to 'Big Brother' temptations and use Web 2.0 networks to spy on own their citizens. The CIA admits openly that it uses Facebook for recruitment purposes, but it would be naïve to believe that states and their intelligence agencies around the world are not using Web 2.0 networks to collect information. Facebook's privacy policy, for example, states that it does not share personal information with third-party companies –but adds that, in order to comply with the law, it may give personal information to 'government agencies'–.

Conclusion: What has radically changed with Geopolitics 2.0 is that old-fashioned state surveillance is now a two-way mirror. Individuals operating in cyberspace can now spy on, and even threaten, their own governments and other states. The shift from states to individuals, from hard to virtual power, and from old to new media has changed the dynamics of global politics forever.

Matthew Fraser
Senior Fellow at INSEAD, Adjunct Professor at the American University of Paris and the Institut d'Etudes Politiques de Paris, and author of 'Weapons of Mass Distraction: Soft Power and American Empire' (2003) and 'Throwing Sheep in the Boardroom: How Online Social Networking Will Change Your Life, Your Work and Your World' (2008)

References

Agence France-Presse (2009), 'Obama Launches "YouTube Diplomacy"', 20/III/2009, http://www.google.com/hostednews/afp/article/ALeqM5jhvOY4aV2-HjBluOVyA2kzPApaPg.

Axe, David (2008), 'Internet Connects Future Army Leaders with Virtual Front Porch', *World Politics Review*, 6/V/2008, http://www.worldpoliticsreview.com/article.aspx?id=2068.

Business Week (2009), 'Iran's Twitter Revolution? Maybe Not Yet', 17/VI/2009, http://www.businessweek.com/technology/content/jun2009/tc20090617_803990.htm

Christian Science Monitor (2009), 'Obama's Strategy to Counter Cyber Attacks', 29/V/2009, http://www.csmonitor.com/2009/0529/p02s09-usgn.html.

IDG News (2009), 'Georgian Cyber Attacks Linked to Russian Organized Crime', 17/VIII/2009, http://www.csoonline.com/article/499778/Georgia_Cyberattacks_Linked_to_Russian_Organized_Crime.

Morozov, Evgeny (2009), 'Foreign Policy: Iran's Terrifying Facebook Police', *Foreign Policy*/NPR, 13/VII/2009, http://www.npr.org/templates/story/story.php?storyId=106535773.

Naim, Moses (2007), 'The YouTube Effect', *Foreign Policy*, January/February, http://www.foreignpolicy.com/users/login.php?story_id=3676&URL=http://www.foreignpolicy.com/story/cms.php?story_id=3676.

Time (2009), 'Tehran's Trials: Blaming the West, Google and Twitter', 8/VIII/2009, http://www.time.com/time/world/article/0,8599,1915399,00.html.

Wall Street Journal (2009), 'US Cyber Infrastructure Vulnerable to Attacks', 6/V/2009, http://online.wsj.com/article/SB124153427633287573.html