Snowden and Unintended Consequences

In November 2013 a delegation of representatives of Russia's Federation Council and Foreign Ministry visited the U.S. with the intention of taking American service providers to task for not guaranteeing user privacy against government intrusion - a reversal of roles which six months earlier would have seemed laughable. But this is just one example of how disclosures by Edward Snowden of alleged U.S. and allied collection and surveillance capabilities have changed the landscape of cyber politics far beyond the post-communist world.

In particular, two important trends have suddenly been accelerated: the legitimisation of surveillance of online activity in a number of countries; and movement towards the establishment of discrete national internets. This is a critical juncture for the future of internet governance worldwide, since the development of both of these trends will be of fundamental importance to those nations which have a stake and a voice in the future of the internet, but which have not yet established a coherent policy on cyber security and internet governance – and consequently, which side of the debate they will join.

Legitimisation

The recent growth of non-Anglophone online populations has led to a rapid movement away from Euro-Atlantic views of the nature of the internet and how it and its freedoms should be regulated. In 1996, the U.S. made up over 66% of the world’s online population, whereas in 2012, it accounted for only 12%. One effect of this shift is an adjustment in median attitudes of internet users to the ideal balance of privacy against security on the internet. The Russian and Chinese approaches to allowing, but controlling, online activity now appear uncomfortably mainstream.

Attempts to shape future governance along former, U.S.-dominated lines - efforts such as the Tallinn Manual on the International Law Applicable to Cyber Warfare and the Global Commission on Internet Governance - are dismissed as Western initiatives which do not reflect the full scope of world opinion on the desired future state of internet governance. Although they may echo the overall attitudes of internet users in the Anglosphere, they are much less reflective of those of internet users overall.

While disclosure of alleged U.S. capabilities provoked widespread reactions of shock in Europe (whether genuine or otherwise), reactions in Russia were tempered by the knowledge that Russia has been operating the SORM monitoring system openly, and governed by laws and regulations which are publicly accessible, for over a decade. In Russia, an online public that is entirely accustomed to being monitored by the state approached the problem with a different set of presumptions. Sampling of opinion among Russian internet users suggests an acceptance of SORM and similar programmes based on greater relative weight given to security concerns over personal
privacy, and an implicit understanding that use of the internet means a renunciation of privacy.

Thus the legality and public acceptability, or otherwise, of covert interception of domestic and foreign telecommunications raises different considerations in different nations. Disappointingly for Snowden supporters, the increase in public debate post-Snowden has led in a number of countries not to a reduction in surveillance, but to its legitimisation through new legal instruments which define and regulate interception. Examples of these states include Sweden, Finland, and France. In the UK, Australia, and to some extent the U.S., this legitimisation takes a different form: open public debate has confirmed the solid legal basis under national law for collection and surveillance activities. Meanwhile, Russia and China feel vindicated in their own approaches to enhancing national security through internet monitoring. One key unintended consequence of the Snowden allegations is therefore a global entrenching of collection and surveillance programmes.

**Internet Sovereignty**

Russia and like-minded nations (for example members of the CIS, CSTO and SCO) strongly support the idea of national control of all internet resources that lie within a state’s physical borders, and the associated concepts of application of local legislation - as described in Russia’s draft Convention on International Information Security, “each member state is entitled to set forth sovereign norms and manage its information space according to its national laws”.

Until Snowden, this was an outlying position, and the notion of national “information space” was primarily a Russian and Chinese concept. Now, support for seceding from the global internet has spread far beyond post-communist countries. For example:

- German Chancellor Angela Merkel has proposed a “communication network inside Europe.”
- Brazil has outlined a number of steps toward a national internet.
- The Philippines, while profusely grateful for U.S. funding for cyber security, are choosing elements of the Russian approach to enforcing it.

The sovereignty principle underlies a key objection to Article 32 of the Council of Europe Convention on Cybercrime (the Budapest convention), which includes the words:

“A Party may, without the authorisation of another Party... access or receive, through a computer system in its territory, stored computer data located in another Party…”
In the Russian view, the phrase “without the authorisation of another Party” is an intolerable infringement on the principle of sovereignty. In addition, the range of options covered by “the person who has the lawful authority to disclose the data” is a source of concern: one Russian analysis calls this a “dubious provision for foreign special services to invade our cyberspace and carry out their special operations without notifying our intelligence services”. Russia proposes instead the Draft Convention referred to above, released in September 2011 during a flurry of intensified diplomatic activity on cyber issues by Russia and China.

Implications and Outlook

In common with other Russian and Chinese initiatives intended to erode the U.S.’s previous near-monopoly on global moral support, WCIT in December 2012 was not an end in itself, but a stage in the long-term process of ticking up support globally for Russian (and by extension Chinese) wishes for internet governance.

Russia and China, and their CSTO and SCO fellow-travellers, are not isolated in their view of information security: there are a large number of other states which share their views. At present, given the congruence between Russian and Chinese approaches and concepts, terminology and policy, it is far easier for Russia, China and like-minded nations to find common ground than it is for English-speaking nations to engage constructively with them. These are groups of states which have already made substantial progress in formalising their shared views on information security. As with other CSTO and SCO initiatives and activities, agreements merely reflect the desires of the organisations’ dominant members. But they nonetheless provide models for other groups of states which are considering a regional approach to cyber security – for example the Gulf Cooperation Council (GCC).

Russian backing of the ITU as a venue mirrors Russian emphasis on the UN as the appropriate forum for a whole range of business. The significance of this to Russia has been summed up as: “The UN system is based on the principle of ‘one state, one vote.’ Hence, if a sufficient number of states want to curtail internet freedoms, the result may be an internet that does not reflect liberal values.”

At the same time the official Russian approach needs to be caveated, since political and security initiatives are at variance with the much more liberal views of the Russian internet industry. For example, the establishment of the new .рф top level domain has been criticised by the Russian industry and activists as establishing a de facto splinternet only accessible to those with Cyrillic keyboards. The Russian authorities possess extremely strong legislative tools for controlling content, but ordinarily apply these with a very light touch. Contrary to perception, many legislators in Russia see the internet as an enabler and excessive restriction as undesirable.

With global opinion divided, the centre of power for deciding the future of the internet is shifting to the undecided nations, which face a choice between the previous Western
multi-stakeholder model, and the state-led model advocated primarily by Russia and China. These nations will need to choose sides or develop independent positions, which risks furthering a gradual online fragmentation into blocs of aligned nations. Thus individual states find themselves playing a greater role, and it is not necessarily the one the West would have chosen for them. Examples include the United Arab Emirates, currently developing its own cyber security strategy and attitude to governance, and investigating the Russian model as an option. There is a significant risk that the global online consensus will shift firmly towards the Russian concept of information security.