Living with cyber insecurity

SREERAM CHAULIA

'I guarantee you that in European capitals, there are people who are interested in, if not what I had for breakfast, at least what my talking points might be should I end up meeting with their leaders. That is how intelligence services operate.'

– Barack Obama[1]

THERE was world politics before anyone knew who Edward Snowden was, and there is world politics after this former contractor for the US National Security Agency (NSA) spilt the beans on the most extensive global Internet-based surveillance operation in history. The sensational revelations and the personal tribulations of the boyish 30 year old computer specialist, who escaped America and lived in suspended animation for weeks before gaining asylum in Russia, have reshaped the very meaning of terms like privacy, security, trust and foreign relations.

Just as the atomic bombings of Hiroshima and Nagasaki in 1945 ushered an unsuspecting world into the nuclear age, Snowden (and his brave predecessors in the WikiLeaks organization) have thrust the planet into the dark unknowns of a cyber insecurity age. After *l'affaire* Snowden, citizens, corporations, non-profit entities and government officials cannot evade the creepy feeling of being followed, watched, hacked into and attacked via cyberspace tools, multiplying a sense of vulnerability and fear like never before. Snowden's detailed expose of the cyber surveillance carried out by the US government and American corporations on a worldwide scale have shattered any semblance of safety and brought war into every connected netizen's consciousness.

Totality is a word that crops up when one looks at PRISM and other top secret American intelligence gathering cyber operations which Snowden uncovered. The very concept of 'metadata' (literally, data about data), which the NSA was collecting like a voracious vacuum cleaner, signifies that military and corporate penetration of everyday lives and definition

1. US President Barack Obama on the storm kicked up by the Edward Snowden saga in Europe.

of politics is now complete. As early as 1999, the Canadian political scientist Reg Whitaker had warned of 'the end of privacy' and the onset of 'total surveillance'. That prediction was before the era of 'web 2.0' technologies, which now render connectivity more social and horizontal, and ensure that the Internet's impact on ordinary lives has multiplied multifold.

Rising Internet accessibility and dependency of all kinds of systems that make up contemporary civilization means that the cyber realm is now the newest and most high impact platform on which politics and conflict are being fought. Concepts like the 'user friendliness' of the Internet means that new cyber politics respects no limits or protocols and can hit any user anywhere. If you have a history and a personality online, you have assets that are now prey to manipulation or destruction by motivated private and public actors.

Welcome to the era of borderless political manoeuvring at the click of a mouse and the application of malicious software. Everyone in this age of cyber insecurity is a potential member of a 'botnet', i.e. a zombie army whose computer could be infected and controlled without the knowledge of its owner by a technically savvy external force. The scariest aspect of this era is that one can be dragged into cyber warfare unwittingly, denying the faculties of human will and volition. Willy-nilly, we are becoming participants in an international political order marked by cyber attacks and counterattacks. War has come closer than our doorsteps; it is in our living rooms and on our fingertips.

The notion of 'anarchy' has predominated theoretical thinking about the nature of the international system for nearly a century. At its simplest, it is a belief that there is no world government (the United Nations is nowhere close to being a coercive global state) and hence might is right in the interactions that take place at the international level. The only guarantee against oppression and subjugation in this Hobbesian 'state of nature' is self-help (through building up one's own material capabilities) or alliances (with a goal of counterbalancing against enemies). Violence or the threat of using force is thus ubiquitous and naturalized in this system.

How would the introduction of a cyber dimension modify or aggravate the anarchic system of world politics? The pessimistic view would hold that web-based weaponry is adding to the conventional and non-conventional military means already in the hands of powerful states and corporations and acting as a force multiplier that can expand the zone of damage in inter-state and inter-corporate rivalries. The fact that only a few countries have managed to develop very advanced cyber offence and cyber defence capacities, while the rest of the world remains a sitting duck that can be attacked at will, magnifies the basic problem of international politics where there are few limits on arm twisting and muscle flexing by the relatively powerful over the powerless.

If one scans comparative spending on cyber security by different regions of the world, it would amplify the point about the gap between the strong and the weak growing larger. According to a new business intelligence report published by Market Research in Delaware, 'The Global Cybersecurity Market 2013-2023', spending in acquiring offensive and defensive cyber weaponry is dominated by North America, with the US government and private sectors being the top clients. North America is projected to shell out $93.6 billion on cyber security in the next one decade. Europe is the second biggest market, projected to spend some US$24.7 billion despite its debilitating continent-wide economic crisis. The Asia-Pacific, which is home to some of the rising powers of the 21st century like China, India, Indonesia and South Korea, is likely to spend around $23.2 billion. The Middle East and Latin America are last in the pecking order, with expected expenditure of $22.8 billion and $1.6 billion respectively.

The above statistics indicate that least developed countries (LDCs) are way behind the cyber arms race, perpetuating the already grim picture of a world in which the big bullies have all the money and firepower. The 'digital divide', which refers to imbalances in availability of the Internet across space and within countries, is therefore taking on another sinister face in the cyber insecurity age.

It is in this context of a widening gap between the haves and the have-nots that one set of controversies generated by Snowden becomes apparent. Some European nations have erupted in fury at learning that they have been in the cross hairs of the NSA's digital tapping behemoth despite having friendly relations with the US. In Germany, where memories of intrusive espionage by fascist and communist dictatorships are not so hoary, Snowden's larger-than-life-size banner was held up by enraged anti-American protesters as a heroic symbol. Further, the bespectacled American was also awarded the 2013 Whistleblower Award in Berlin. German citizens and lawmakers demanded apologies from the US government, and the issue of Germany standing up to big brother America even made a mark on the election campaign for the chancellor's office in September 2013.

What baffled Europeans, including the European Union institutions whose communications were all bugged by the NSA, was that the Barack Obama administration was using the alibi of deterring terrorist attacks for its cyber surveillance over routine diplomatic and commercial exchanges that had nothing to do with Al Qaeda or any such violent organization. President Obama's retort, that the Europeans also spy on the US using cyber means, and that such activity is standard procedure for gauging 'talking points' of each other prior to bilateral or multilateral negotiations, does not take away from the asymmetry in cyber offence and defence capabilities between the US on one hand, and the entire EU's 28 members put together. As combined European spending is likely to remain far below that of the US alone in the next decade, cyber snooping will mostly be one-sided and the advantages of surprising partners in trade and military talks will remain firmly in American hands.

The pervasive inequality that underlies the anarchic world order gets even starker if one looks at how Snowden's bombshell has impacted relations between the US and Latin America. Brazilians reacted in a collective burst of anger when Snowden's tranche of leaks showed that millions of their emails and phone calls were indiscriminately subjected to cyber hacking and tapping by the NSA. Brazil's President Dilma Rousseff had to express 'indignation' at this violation of privacy and sovereignty and there were attempts to launch criminal proceedings against the US government. On learning that the American cyber army was hacking into computer systems of Petrobras, Brazil's state-owned oil major, President Rousseff echoed what the Europeans said by commenting that, 'It's evident that the motive for the espionage is not security or to fight terrorism, but economic and strategic interests.'

The willingness of left-ruled Latin American governments of Bolivia, Nicaragua and Venezuela to offer asylum to Snowden reflects how central cyber warfare is in drawing battle lines in international politics today. The President of Bolivia, Evo Morales, was humiliated mid-air when his plane was diverted on suspicion that he was carrying Snowden to safety from his hideout in the Moscow airport, drawing harsh condemnation across Latin America that the US and its European allies were committing an 'act of aggression' and 'an offence against the whole Latin region.' Seen from a historical lens, such crude US intelligence attempts to nab Snowden rubbed salt into the wounds of a Latin America that nurses old grievances about American meddling and divide-and-rule strategies. Cyber hacking is showing a barometer or mirror to the anti-Americanism that drives radicalized parts of the world. The ease with which computers can be hijacked and purloined if one's cyber defences are not up to date and cutting edge is bound to sow angst and despair in materially weaker nations and regions that are striving to banish neocolonial chokeholds.

From friendly nations to hostile ones, people are realizing that the US, or for that matter no country, can be trusted to respect their sovereign rights. It reinforces the image of a world where morals and laws have been trampled by the logic of endless power accumulation and expansion. Cyber insecurity has obliterated rhetorical distinctions between freedom-promoting liberal powers and repressive authoritarian states. Regardless of whether a country is democratic or dictatorial, everyone hacks as mercilessly as the cyber expertise at hand permits in pursuit of what President Rousseff terms 'strategic interests'. Civilized behaviour, which was always a convenient mask for depravity in the international system, has been dealt a death knell by strategic deployment of cyber weaponry.

While Europe and Latin America are, as yet, weak in countering the US through tit-for-tat cyberspying and attacks, the response of relatively capable cyber powers like China and Russia to the Snowden fallout are indicative of the future balance of power that holds out hope against the anarchic rule by brute force in the international system. Washington was miffed at the role the Chinese government played when Snowden landed in Hong Kong with the intention of giving American law enforcers the slip. Despite repeated entreaties by the US government to hand over Snowden, the Chinese authorities decided to exploit him to their own advantage and to pay back the embarrassment that the Americans had been piling up through evidence against China's aggressive cyber attacks for the last few years. The perpetual accuser of China's hacking and cyber stealing of industrial secrets was now standing in the dock of global public opinion, and the nationalistic Chinese elites and citizens extracted maximum mileage by parading Snowden as a crusader for justice against the American empire.

China's decision to let Snowden fly to Russia, and rumours that the Russians contacted and assisted him while he was still lying low in Hong Kong, suggests coordination between Beijing and Moscow to counter Washington at a broader political level. Since both China and Russia have been under relentless western media and governmental pressure regarding human rights abuses and denial of per-

sonal freedoms to their citizens, the Snowden issue was a device for governments in Beijing and Moscow to turn the tables on Washington for its own intolerance of conscientious whistleblowers who opposed American military hegemony around the world. The Chinese state-run mouthpiece, *Global Times*, also used the opportunity to argue that 'the Internet is changing the world' and that a great 'fight' against Washington's hypocrisy regarding civil and political rights has begun.

Interestingly, although China and Russia rebuffed the US and ultimately helped to hide Snowden from those hunting for him in western intelligence circles, there were plenty of nuances in the language used by both these anti-western powers so as to not offend the US beyond a point. Russian President Vladimir Putin appeared to be as conciliatory as publicly possible towards America by saying at one point that for Snowden to remain in Russia, he 'must stop his work aimed at harming our American partners.' But behind the scenes, both Chinese and Russian cyber war teams definitely disgorged whatever relevant information they would have needed from Snowden's four laptop computers while he was first in Hong Kong and since then in some undisclosed location in Russia. The *realpolitik* lesson that hard-headed leaders like President Xi Jinping and President Putin would have learnt from the episode is to assess how far and deep American cyber warfare has advanced and to match it through research by their own indigenous cyber legions.

While China's prowess in cyber spying and cyber attacks is widely known due to western counter-intelligence efforts as well as alarms raised by affected Asian rivals like India and Japan, Russia is no one's inferior in this latest theatre of warfare. In 2007, when the technology to wage war via the Internet was still developing, Russia was accused of launching a three week long blitz of cyber attacks on the tiny Baltic state of Estonia, disabling websites of government ministries, news media, corporations, banks and political parties. The government of the Caucasian country, Georgia, also alleged that Russia launched cyber attacks on its critical infrastructure simultaneous to an actual physical military attack in August 2008. The Georgian Ministry of Justice concluded from this bitter experience that 'cyberspace is a war space'. Private Russian hackers are also hyperactive in the world of cyber crime, setting up a parallel and sometimes intersecting web with the national security apparatus of the Russian state.

Apart from China and Russia, the other big player that has emerged with cyber warfare capabilities is Israel. The fact that Israel has a strong indigenous military-industrial base has helped it to build a sophisticated range of cyber offence and defence weapons. The Israeli Army has invested heavily in cyber warfare and Prime Minister Benjamin Netanyahu has set a goal for his country to turn into a 'world cyber power'. The sensational cyber attacks that slowed Iran's controversial nuclear programme and which were code-named Operation Olympic Games were the handiwork of Israeli intelligence working in coordination with the Americans. The Stuxnet computer worm, which was the key striking agent of Olympic Games, had a devastating impact on not just Iranian strategic sites but also infected thousands of computer systems in India and Indonesia. It was the equivalent of a cyber weapon of mass destruction (WMD) and a sign of the havoc that is to come as virtual attacking technology gets more sophisticated.

Is there no liberal solution to clear the darkening skies of cyber insecurity driven by cut-throat inter-state competition and corporate drive for profits? Can the mayhem not be limited through international treaties or conventions? Can the 'geek space' be preserved from being converted into what Rex Hughes of Cambridge University labels the 'fifth battle space' in which the worst human trait of violence is reigning? There is already a Budapest Convention that binds the international community to cooperate in rooting out cyber crime. Can sanity not prevail and usher in something similar to mitigate cyber WMDs that are crippling normal life on a worldwide scale? Russia has proposed an international 'code of practice' under the aegis of the UN to control 'misuse of information technologies against individual states and the world as a whole.'

But movement towards consensus is proving chimeric because western notions of cyber security are at odds with Russian and Chinese calls for 'information security', a broader phrase that covers curbing the content of the worldwide web. Also, the relative lead that the US enjoys over the rest of the major powers in cyber war capabilities means that Washington is least interested in a multilateral treaty-bound regime to monitor and restrict its freedom to attack and spy at will. In late 2012, the US objected to expanding the mandate of an international telecommunications treaty relating to cyber security on the ground that countries need to be agile enough to respond to cyber attacks on their critical infrastructure.

In other words, the flexibility that a leading cyber power has at its hands to mete out punishment and dictate terms to other nations is at risk if cyber war is subjected to international regu-

lations. The impetus for a global convention is therefore more likely to come from smaller cyber powers and cyber non-powers which are most at risk of destabilization. As the history of the Rome Statute that formed the International Criminal Court shows, it is possible for a cyber security regulatory regime to be formed even without the participation of the US. But the absence of the US will act as a negative contagion and compel China, Russia and other cyber powers to also opt out of a binding international treaty out of a justified fear that subjecting themselves to laws while the big bully is free to misbehave is suicidal.

Meanwhile, victims of cyber war like India are entering into bilateral cyber security agreements with the US for exchange of information and techniques between nodal agencies handling web-based threats. India, which was one of the first countries to establish a formal command and control (C2) over military assets in the cyber domain, is nonetheless a firm believer in the doctrine of self-reliance. India's premier electronic warfare agencies are skeptical that the Americans would ever share technology and data beyond what serves narrow American interests. Indian technocrats handling cyber warfare have often expressed disappointment that the Americans deliberately withhold timely leads that could make a crucial difference for India's national security. The cyber war between China and India is so acute and independent of the swings in relations between Washington and Beijing that New Delhi is determined to be a cyber power through its own indigenous investments and coordination with India's software giants.

Notwithstanding the hierarchy of cyber powers in international politics, the Internet can also be a great leveller by empowering smaller actors. The way in which Iran, Syria and North Korea have struck western assets through their own computer viruses, and the possibility of violent non-state guerrilla groups also utilizing cyber weaponry for propaganda hits, means that relative capabilities do not explain the entire structure of cyber insecurity. The fact that the US, China, Russia and Israel are themselves not foolproof from repeated cyber attacks means that we have entered a dangerous new phase of world politics where the source of warfare is not easy to trace and the damage suffered is not simple to calculate. The cyber insecurity age is one where politically motivated hackers unions like Anonymous can quickly make their points even if they lack the weightiness of cyber commands of almighty powers like China or the US. It is a world where everyone is afraid and paranoid.

The only positive news emanating from the cyber insecurity age is that the 'leveller' function of the Internet also enables social justice and anti-war platforms such as WikiLeaks and builds mass revulsion against war and skulduggery of great power politics. One can hope that this contrapuntal growth of activism in cyber space for progressive causes like world peace and exposing misdeeds of the powerful will eventually beat back the violence and the naked profiteering that states and their private sector allies have been engaging in via cyber weapons.

If the Internet does succeed in bringing the average citizens of the world together into a grand coalition against war, dictatorship and inequality, then it may have offered the perfect antidote to the fear and loathing that state intelligence agencies and corporate warriors have been spreading in the cyber domain.