theguardian | TheObserver

How cryptography is a key weapon in the fight against empire states

What began as a means of retaining individual freedom can now be used by smaller states to fend off the ambitions of larger ones

Julian Assange

guardian.co.uk, Tuesday 9 July 2013 12.45 BST

The original cypherpunks were mostly Californian libertarians. I was from a different tradition but we all sought to protect individual freedom from state tyranny. Cryptography was our secret weapon. It has been forgotten how subversive this was. Cryptography was then the exclusive property of states, for use in their various wars. By writing our own software and disseminating it far and wide we liberated cryptography, democratised it and spread it through the frontiers of the new internet.

The resulting crackdown, under various "arms trafficking" laws, failed. Cryptography became standardised in web browsers and other software that people now use on a daily basis. Strong cryptography is a vital tool in fighting state oppression. That is the message in my book, Cypherpunks. But the movement for the universal availability of strong cryptography must be made to do more than this. Our future does not lie in the liberty of individuals alone.

Our work in WikiLeaks imparts a keen understanding of the dynamics of the international order and the logic of empire. During WikiLeaks' rise we have seen evidence of small countries bullied and dominated by larger ones or infiltrated by foreign enterprise and made to act against themselves. We have seen the popular will denied expression, elections bought and sold, and the riches of countries such as Kenya stolen and auctioned off to plutocrats in London and New York.

The struggle for Latin American self-determination is important for many more people than live in Latin America, because it shows the rest of the world that it can be done. But Latin American independence is still in its infancy. Attempts at subversion of Latin American democracy are still happening, including most recently in Honduras, Haiti, Ecuador and Venezuela.

This is why the message of the cypherpunks is of special importance to Latin American audiences. Mass surveillance is not just an issue for democracy and governance – it's a geopolitical issue. The surveillance of a whole population by a foreign power naturally threatens sovereignty. Intervention after intervention in the affairs of Latin American democracy have

taught us to be realistic. We know that the old powers will still exploit any advantage to delay or suppress the outbreak of Latin American independence.

Consider simple geography. Everyone knows oil resources drive global geopolitics. The flow of oil determines who is dominant, who is invaded, and who is ostracised from the global community. Physical control over even a segment of an oil pipeline yields great geopolitical power. Governments in this position can extract huge concessions. In a stroke, the Kremlin can sentence eastern Europe and Germany to a winter without heat. And even the prospect of Tehran running a pipeline eastwards to India and China is a pretext for bellicose logic from Washington.

But the new great game is not the war for oil pipelines. It is the war for information pipelines: the control over fibre-optic cable paths that spread undersea and overland. The new global treasure is control over the giant data flows that connect whole continents and civlisations, linking the communications of billions of people and organisations.

It is no secret that, on the internet and on the phone, all roads to and from Latin America lead through the United States. Internet infrastructure directs 99% of the traffic to and from South America over fibre-optic lines that physically traverse US borders. The US government has shown no scruples about breaking its own law to tap into these lines and spy on its own citizens. There are no such laws against spying on foreign citizens. Every day, hundreds of millions of messages from the entire Latin American continent are devoured by US spy agencies, and stored forever in warehouses the size of small cities. The geographical facts about the infrastructure of the internet therefore have consequences for the independence and sovereignty of Latin America.

The problem also transcends geography. Many Latin American governments and militaries secure their secrets with cryptographic hardware. These are boxes and software that scramble messages and then unscramble them on the other end. Governments purchase them to keep their secrets secret – often at great expense to the people – because they are correctly afraid of interception of their communications.

But the companies who sell these expensive devices enjoy close ties with the US intelligence community. Their CEOs and senior employees are often mathematicians and engineers from the NSA capitalising on the inventions they created for the surveillance state. Their devices are often deliberately broken: broken with a purpose. It doesn't matter who is using them or how they are used – US agencies can still unscramble the signal and read the messages.

These devices are sold to Latin American and other countries as a way to protect their secrets but they are really a way of stealing secrets.

Meanwhile, the United States is accelerating the next great arms race. The discoveries of the Stuxnet virus – and then the Duqu and Flame viruses – herald a new era of highly complex weaponised software made by powerful states to attack weaker states. Their aggressive first-strike use on Iran is determined to undermine Iranian efforts at national sovereignty, a prospect that is anathema to US and Israeli interests in the region.

Once upon a time the use of computer viruses as offensive weapons was a plot device in science fiction novels. Now it is a global reality spurred on by the reckless behaviour of the

Barack Obama administration in violation of international law. Other states will now follow suit, enhancing their offensive capacity to catch up.

The United States is not the only culprit. In recent years, the internet infrastructure of countries such as Uganda has been enriched by direct Chinese investment. Hefty loans are doled out in return for African contracts to Chinese companies to build internet backbone infrastructure linking schools, government ministries and communities into the global fibre-optic system.

Africa is coming online, but with hardware supplied by an aspirant foreign superpower. Will the African internet be the means by which Africa continues to be subjugated into the 21st century? Is Africa once again becoming a theatre for confrontation between the global powers?

These are just some of the important ways in which the message of the cypherpunks goes beyond the struggle for individual liberty. Cryptography can protect not just the civil liberties and rights of individuals, but the sovereignty and independence of whole countries, solidarity between groups with common cause, and the project of global emancipation. It can be used to fight not just the tyranny of the state over the individual but the tyranny of the empire over smaller states.

The cypherpunks have yet to do their greatest work. Join us.

9 July 2013
From www.guardian.co.uk/commentisfree/2013/jul/09/cryptography-weapon-fight-empire-states-julian-assange