PHYS.ORG

To avoid militarising the internet, cyberspace needs written rules agreed by all

June 3 2015, by Brandon Valeriano

There needs to be rules that govern what takes place in the cloud as there are for what occurs on the ground. Credit: David James Paquin

In the world of foreign affairs, there are written or unwritten rules – behavioural norms – under which states operate. But there is little, if any, comparable set of structures governing actions taken in cyberspace. As this becomes a larger and more important part of life and the security implications that arise, this poses a problem.

The US government recently released its strategy for cyberspace, the fourth update since 2010. Britain did the same in 2011 and again in 2013. The aim of the documents aim is to outline the consequences of foreign actions taken in cyberspace in order to provide a deterrent to their use. The problem is, that in order to promote an international norm that could be agreed upon, any global strategy should really be drawn up by a state that hasn't already launched cyber-attacks.

For example, the US strategy document lists China, Russia, Iran, and North Korea as its prime digital enemies. The research that Ryan C Maness at Northeastern University and I undertook for our book on cyberwarfare found 20 attacks by China on the US from 2001-2011, three by Russia, one by Iran, and three by North Korea. After 2011, there have been Russian intrusions into the White House and Department of State, Iran's attack on Saudi Arabia in 2012, and North Korea's attack on Sony in 2014.

What is needed is a set of understood norms that specify the consequences of offensive actions taken in cyberspace. According to the US strategy, around 2% of the cyber attacks listed would invite a military response since they are of a significantly offensive nature, rather than merely inconveniences. Unfortunately, these statements alone would not be a deterrent. A military response may be an option for the US, but ultimately such threats are deemed empty without a demonstrated commitment to carry them out.

This is the classic nuclear dilemma covered so well in Dr Strangelove. How could any nation be sure another would commit to retribution in a given situation? Consequences are not a sure thing – as Syria discovered with the US's moving "red line" in relation to chemical weapons. Suggesting that the evidence was not at all definitive, the US declined to launch an attack because it cannot be sure that Syrian president, Bashar al-Assad, condoned the attacks.

Cyber attacks prompt even deeper questions, as attribution is very difficult – and, even then, knowing who is responsible is of limited value when launching a conventional strike. Just because certain actors within a country might be responsible for an attack does not mean that the nation should be held accountable and punished.

A proper global cybersecurity strategy would need to move beyond consequences and threats towards a greater consideration of norms that could provide a basis for a collective response to the violation of agreed rules. These could include the limitation of physical damage, an agreement that civilians and civilian infrastructure are off-limits and to keep critical infrastructure such as power or water supply out of bounds in order to avoid the potential for humanitarian disasters.

But it's tough for the US to call for military responses to cyber attacks when it is itself linked to nine such attacks between 2001-2011, including deploying the Stuxnet malware on Iran, the most advanced attack to date – not to mention all the revelations of the Snowden files. Other European nations can play a role here: with little connection to cyber-attacks, they could take a hand in outlining the future rules of the game without being hamstrung by obvious claims of hypocrisy and hidden agendas.

Cyberspace is the natural domain of research, education, social interaction and commerce. As far as is possible it needs to avoid militarisation. A just and proper strategy for cyberspace cannot be left to the aggressors or the victims to define – it is in the interest of all that every nation state contributes their voices.

Source: The Conversation

Citation: To avoid militarising the internet, cyberspace needs written rules agreed by all (2015, June 3) retrieved 17 April 2024 from https://phys.org/news/2015-06-militarising-internet-cyberspace-written.html