Opinion: Diplomacy, not sanctions, are needed to tackle state cyberespionage

September 15 2015, by Ryan C Maness And Brandon Valeriano

More jaw jaw, less war war. Credit: Ad Meskens, CC BY-SA

The war of words between China, Russia and the US has escalated recently with the White House declaring its intention to apply sanctions in response to what the US sees as state-sponsored cyberattacks from the

east.

So far in 2015, Russia been implicated in hacks of the IRS, the the White House, the Joint Chiefs, and the State Department.

China has been named the culprit for the hack of the Office of Personnel Management, which stole the personal records of nearly 21m US citizens. The two countries are now reportedly working together in the difficult work of deciphering the raw data from these hacks.

The proposed sanctions may target individuals and corporations – some of whom are likely to be close to the governments of both countries – for their role. The problem with confronting Russian moves in cyberspace is that using the tool of economic sanctions is virtually toothless and ineffective given what we know about Russia and sanctions. China may be an entirely different story, given its current economic problems and high interconnectedness with the global economy, but Russia stands better able to defy Western sanctions. The declining price of oil has hurt more than sanctions ever could, and Russia is not central to the global economy.

Russia is already in decline and confronting Russia's leadership now will demand a response. With the continuing stalemate in the civil war in Ukraine, Russia has backed itself into a corner and has no easy way out. It has already been sanctioned for its actions in Ukraine, which include arming the separatists and sending in Russian regulars to fight alongside the rebels in Donbas. Yet these sanctions have only emboldened the Kremlin to see the conflict through to the very end and made Vladimir Putin more popular at home for his tough stance against the West.

Espionage vs cyberespionage - tactics are different, but the game is the same. NSA

So with this in mind, what good would sanctioning Moscow again for hacking computer networks do? Sanctions are an ineffective tool to deal with cyberspace disputes. They do not go to the root of the problem, which lies in nature of espionage and the oversights or weaknesses in securing our own networks. The fact that many government networks are still using 14-year-old Windows XP suggests that much of the blame lies with our own governments' ineptitude. Huge vulnerabilities such as these are invitations to hackers of any sort. We should shore up our defence before finding a way to respond, to do otherwise is premature.

Bring everyone into the tent

Why do sanctions often fail, especially if against individuals and companies? To have any effect sanctions must be comprehensive, giving those sanctioned no other avenues to access the resources they're denied. When sanctions are targeted and unilateral, this can be hard to achieve. It has been over a year since the Department of Justice indicted five People's Liberation Army officers for cyber-espionage, yet China continues its campaigns against US networks.

Sanctioning Russian individuals or companies would not stop Moscow from continuing to exploit the continued vulnerabilities found in US networks without the support of the entire international community and a willingness to target the entire country. Of course, reaching international agreements is complicated by the fact that the US is also a major player in the game of international cyber-espionage, and Russia and China feel that if their cyberspace is violated by the US then they are justified in responding.

The cyberspace domain has existed for more than 25 years: these are not new threats or methods of attack – and confronting these problems with traditional sanctions fails to recognise their limitations when applied to this domain. Two steps are needed to confront Russia: achieve a workable framework for stability in Ukraine and develop rules and norms in cyberspace to regulate the constant violations that are considered part of spycraft.

There is evidence that we have done much to develop a system that might work for China. Just recently, senior Chinese and US officials have held talks to discuss cybersecurity issues ahead of Chinese president Xi Jinping's official visit to Washington. But Russia is often left out of the picture. Russia must be brought into the international community and participate in developing a system of regulation for

cyberspace. Russia should be included in the process of considering what cyber-laws might be, but currently this is impossible as this effort is centred in Tallinn, Estonia, which left post-Cold War Russia for NATO.

This is not a call for greater respect of Russia, but a call to respect every stakeholder in the international system as we try to figure out what is allowed in world of constant cyber-threats. Excluding a major state actor only insures they will do what they can to undermine any new framework.

Escalation is not the answer. Sanctions are weak and ineffective. They make us feel like something is being done even though the moves are generally regressive and target innocent civilians. "Smart sanctions" are just a buzzword. Those that feel the need to apply sanctions need to face up to their own inefficiencies in defence, their inadequacy of offence, and the weakness of any sanctions regime in achieving their aims.

There are no quick fixes, only concerted action by the entire international community will establish the rules for the cyberspace world.

Source: The Conversation