We need new laws to govern cyberwarfare

August 21 2014, by Bela Bonita Chatterjee

Mouses not guns, a future view of the battlefield. Carrie Kessler/USAF

President Bush is reported to have said: "When I take action, I'm not going to fire a US$2m missile at a US$10 empty tent and hit a camel in the butt. It's going to be decisive." As the quote suggests, when it comes to national defence, enemies are unlikely to be deterred by an army of three, a leaky canoe and a fleet of second-hand microlights. In times of war we usually expect a powerful, graphic display of military might.

Nations may feel reassured that the sheer scale and sophistication of their armed forces will be enough to deter any potential threat, with would-be attackers put off by the mere prospect of retaliation. But what

if decisive action can be conducted without armed forces, without firing a single bullet, but by simply pressing "enter"?

This is the promise of cyber-warfare, where the hostile use of software against a state's critical infrastructure such as energy and transport networks, financial markets, hospitals, can have immediate and devastating effects. The tools of cyber-warfare could be acquired with relative ease by new belligerent nations who were hitherto considered unthreatening by virtue of their lack of conventional forces. Belligerents may not even be nations, but unaffiliated hackers driven by a common political, religious or economic ideology, who can quickly form, strike and disperse using the anonymity of the internet to hide their tracks.

Nations have had to take the threat of cyber-warfare seriously. Several significant military powers have now publicly declared policies on cyber-warfare, and the topic has dominated diplomatic exchanges at the highest level. Perhaps the most poignant acknowledgement of cyber-warfare as a serious issue comes from its inclusion as a topic of importance in the 2011 Report of the International Red Cross on International Humanitarian Law and the challenges of contemporary armed conflicts.

The growing recognition of cyber-warfare as a topic of legal concern in particular is of great importance, particularly for international law, which, among other things, it sets out a framework for the legally permissible use of force. International Humanitarian Law (also known as the Law of Armed Conflict) is the part of international law which tries to ensure that if there is armed conflict, it is conducted in as humane and restrained a manner as possible.

Determining how legal rules apply to cyber-warfare is obviously important. States will want to know whether cyber-offensives will come under the rules of international law, what limits may be applied and what

action can be taken in response within the law. If a cyber-war is unavoidable, then states will also want to know what rules apply to the actual conduct of such war, for example in determining what targets are permissible, how rules on neutrality apply, and what kinds of cyber-weapons are permissible.

However, there is a lack of clarity on how international law applies to cyber-warfare. International law has evolved over time and is heavily influenced by traditional concepts of conventional armed warfare between clearly defined nation states. Cyber-warfare is so new it is not specifically addressed in any treaties. It is difficult enough to reach an agreement on international matters at the best of times, especially in dealing with conflicts. This difficulty will undoubtedly apply to cyber-warfare too.

In light of this considerable uncertainty, a recent report for Security Lancaster outlines an agenda for future legal research on cyber-warfare. This calls for a reconsideration of whether international law is a useful framework. For example, international law focuses heavily on states, but are future cyber-attacks likely to come from states themselves? How should cyber-hostilities initiated by federated or balkanised hacker groups with no clear state affiliation be legally categorised? Would we be better off starting to construct a legal framework from scratch as opposed to one built around outdated concepts that no longer reflect the current military realities?

It should be acknowledged that not all share the view that cyber-warfare is a significant or worrying prospect. Its detractors point out that it has been responsible for no human casualties to date, and no hostile cyber-incident has as yet been treated as an act of war or openly admitted to by a state. But this ought not to deter us from taking the issue seriously, and to start thinking about an acceptable – and perhaps more importantly, workable – legal framework to cover the resort to and conduct of cyber-

warfare.

We would do well to recall that another world leader, Winston Churchill, was widely derided at the time for forecasting the onset of World War II, and remember that if the lessons of history are not learned they are destined to be repeated. If World War III promises to be digital, we must be as prepared as we can be.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation