This article is the fifth in a five-part series exploring Australian national security in the digital age. Read parts one , two , three and four here.

As technology evolves and Australia becomes ever-more reliant on cyber systems throughout government and society, the threats that cyber attacks pose to the country's national security are real – and significant.

Cyber weapons now exist that can be used to attack and exploit vulnerabilities in Australia's national infrastructure. Many of the cyber threats that exist now, such as defacing a website, are not that serious.

But more nefarious attacks on software systems have the potential to damage critical infrastructure
and threaten people's lives.

Read more: ***Since Boston bombing, terrorists are using new social media to inspire potential attackers***

The Australian Cyber Security Centre (ACSC) Threat Report addresses these concerns every year, highlighting the ubiquitous nature of cyber-crime in Australia, the potential for cyber-terrorism, and the vulnerability of data stored on government and commercial networks.

Governments now take these types of threats so seriously, they speak of the potential for military responses to cyber-attacks in the future. As one US military official told The Wall Street Journal :

If you shut down our power grid, maybe we will put a missile down one of your smokestacks.

A securitised internet

Such concerns have been a key part of Australia's ambitions to revamp its national security to respond to future cyber-threats. Australia’s Cyber Security Strategy , for instance, states that:

all of us – governments, businesses and individuals – need to work together to build resilience to cybersecurity threats and to make the most of opportunities online.

An important ethical concern with such a focus, however, is the risk that Australia's cyberspace becomes "securitised".

When we securitise an issue, we frame the activity as being conducted in a state of emergency. A state of emergency is when a government temporarily changes the conditions of its political and social institutions in response to a particularly serious emergency. This might be a natural disaster, war or rioting, for example. Importantly, due process constraints on government officials, such as *habeas corpus* , are suspended.

An ethical problem with a securitised or militarised cyberspace, especially if it becomes a permanent measure, is that it can quickly erode fundamental human rights such as privacy and freedom of speech.

Ethical problems in a brave new world

For instance, what are the ethical implications of conducting military activities against terrorist propaganda online, by conducting psychological operations on social media platforms, say, or simply shutting them down?

Using social media in this way would be counter to the social and civil function of these channels of communication. Trying to deny audiences the ability to speak freely on social media

could also undermine the internet's effectiveness as a tool for social and economic good. This is especially problematic in Australia, where fundamental human rights such as privacy and freedom of speech are taken for granted as fundamental civic values.

There is also potential for a militarised cyberspace to increase the likelihood of conflict between states. As cyber-attacks are a relatively new threat, it's unclear what actions might lead to escalation and constitute an act of war.

The perception that cyber-attacks are not as harmful as, say, a missile attack could lead to their increased use. This opens the door to potentially more serious forms of conflict.

Read more: ***The Cyber Security Strategy is only a small step in the right direction***

Another important ethical consideration is the enhanced government surveillance of a securitised internet. The fall-out from the Edward Snowden disclosures, for instance, revealed the intrusiveness of US security agencies’ activities online. This in turn had the effect of undermining the public’s trust in the government.

Such a loss of trust in one segment of the government can have potentially dire impacts on other areas. For example, in response to public suspicions of the actions of security agencies, governments might overreact and cut worthwhile surveillance programmes. Or disgruntled government employees (like Snowden) might leak other types of confidential or sensitive information to the detriment of the public good.

A recent example of this occurred when highly sensitive correspondences between Home Affairs Secretary Mike Pezzullo and Defence Secretary Greg Moriarty were leaked to the media. The communications detailed plans to give the Australian Signals Directorate new

domestic surveillance powers. Mark Dreyfus, the national security shadow minister, labelled the leak , “a deeply worrying signal of internal struggles.”

So it is important that Australian government agencies tasked with managing national security in cyberspace consistently act in a trustworthy manner. As such, there should be guarantees that decisions related to cyber-security oversight and governance are not driven by short-term political gains.

In particular, government decision-makers should seek to promote an informed and public debate about the standards required for “minimum transparency, accountability and oversight of government surveillance practices.”

Anything short of that could make the country’s cyber-infrastructure less secure – a frightening prospect in an increasingly hostile and volatile digital world.

Dr Shannon Brandt Ford receives funding from the Australian Army Research Scheme.

Authors: Dr Shannon Brandt Ford, Lecturer, Curtin University

Read more http://theconversation.com/the-ethics-of-securitising-australian-cyberspace-95523