Efforts to control cyber weapons ignore the agents who use them

February 15 2019, by Alexi Drew

Credit: AI-generated image (disclaimer)

Reports of malicious and targeted cyber attacks are becoming increasingly common around the world. In early February, for example, Australia's security agencies revealed there were investigating an attempted hack on the country's parliament, and hadn't ruled out another country being behind it.

As more complex and potentially damaging attacks into critical national infrastructure systems are discovered, calls are growing louder for international rules to govern this emerging battlefront.

Efforts towards cyber-arms control have predominantly centred around a model where the "arms" relates to weaponised code – specific hacking tools or the software vulnerabilities that enable them. Attempts have been made to curtail the proliferation and spread of what are called "zero-day exploits" – the flaws in a program's code that allow malicious attackers to interfere with the systems that run them.

A recent Reuters expose of the operations of a clandestine wing of the United Arab Emirates' (UAE) National Electronic Security Authority (NESA) exposed another component of offensive cyber-attacks – expertise. This issue sparked further international attention when the FBI announced charges in mid February against Monica Witt, a former US Air Force analyst, accused of espionage and defecting to Iran.

Cyber mercenaries

The Reuters investigation detailed how some former employees of the US National Security Agency (NSA), operatives with expertise in digital penetration techniques, online intelligence gathering and offensive cyber-operations, were contracted via a Maryland-based firm to work for the UAE.

The investigation makes specific mention of one of the tools – Karma – that these contractors employed on behalf of the UAE against specific targets. This hacking tool allowed its operators to gain uninvited and remote access to a target's Apple phone through an unspecified flaw which is now believed to have been fixed by Apple. Reuters reported that the targets of these attacks ranged from human rights activists, to American journalists.

The article raised questions about whether these contractors might have provided their NESA employees with advanced cyber-capabilities developed by their former employer, the NSA. But the subtext of the Reuters investigation is that the expertise of these former intelligence officers is just as attractive to their new employers as any tools they might bring with them.

In a separate article, specifically examining Karma, Reuters alleges that it was purchased by the Emirati government from a vendor outside of the country. In effect, the UAE had hired a team of out-of-work specialist engineers who couldn't bring the tools they had used in the US with them, so it then bought them the tools they needed to get the job done. This suggests that there are two components required to kit out any state or group with advanced cyber-capability: the tools and the expertise.

Tools and expertise

Global efforts are underway to govern the tools used in cyber attacks, such as the Global Commission on the Stability of Cyberspace, which introduced a series of international norms about the use of cyberspace to promote the stability of the internet and good practice of everyone involved. Other efforts have been on the the legislative level, such as specific additions to the Wassenaar Arrangement, an export control arrangement that seeks to curtail the spread of civilian technologies that can be put to militarised use. But the expertise of cyber operatives has so far seen limited attention.

In the scenario described by Reuters, NESA and its Project Raven could not have operated without either the tools or the expertise. The tool itself – Karma – and the expertise and experience required to use it and train others to do so, both require significant investment.

The dangers of state investment in the collecting of software flaws and the creation of powerful tools which then exploit these previously unknown weaknesses was painfully demonstrated through the leaking of the vulnerability stockpiled by the NSA, EternalBlue. This was the backbone of the WannaCry attack which made international headlines in 2018 through its impact on the British NHS and other international business and government services.

But concerns should be growing about the capability that states invest in the skill sets of the people who discover and then weaponise flaws in the software which power our increasingly interconnected and internet-dependent lives. Governments across the world are gearing up for what they see as the next domain of warfare by trying to recruit existing talent to government projects or through training the next generation of cyber-security experts who they hope will give them an advantage.

There's a risk that in global efforts which focus on states' use of cyber tools and exploitation of vulnerabilities in programming code, there is a legislative and governance gap developing. This could see states invest in training the cyber spies, saboteurs or soldiers of the future only to find those critical skills and the capability they provide being snapped up by the highest bidder.

Provided by The Conversation