THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Spectrum automation

Legal challenges of optimising spectrum use for military operations

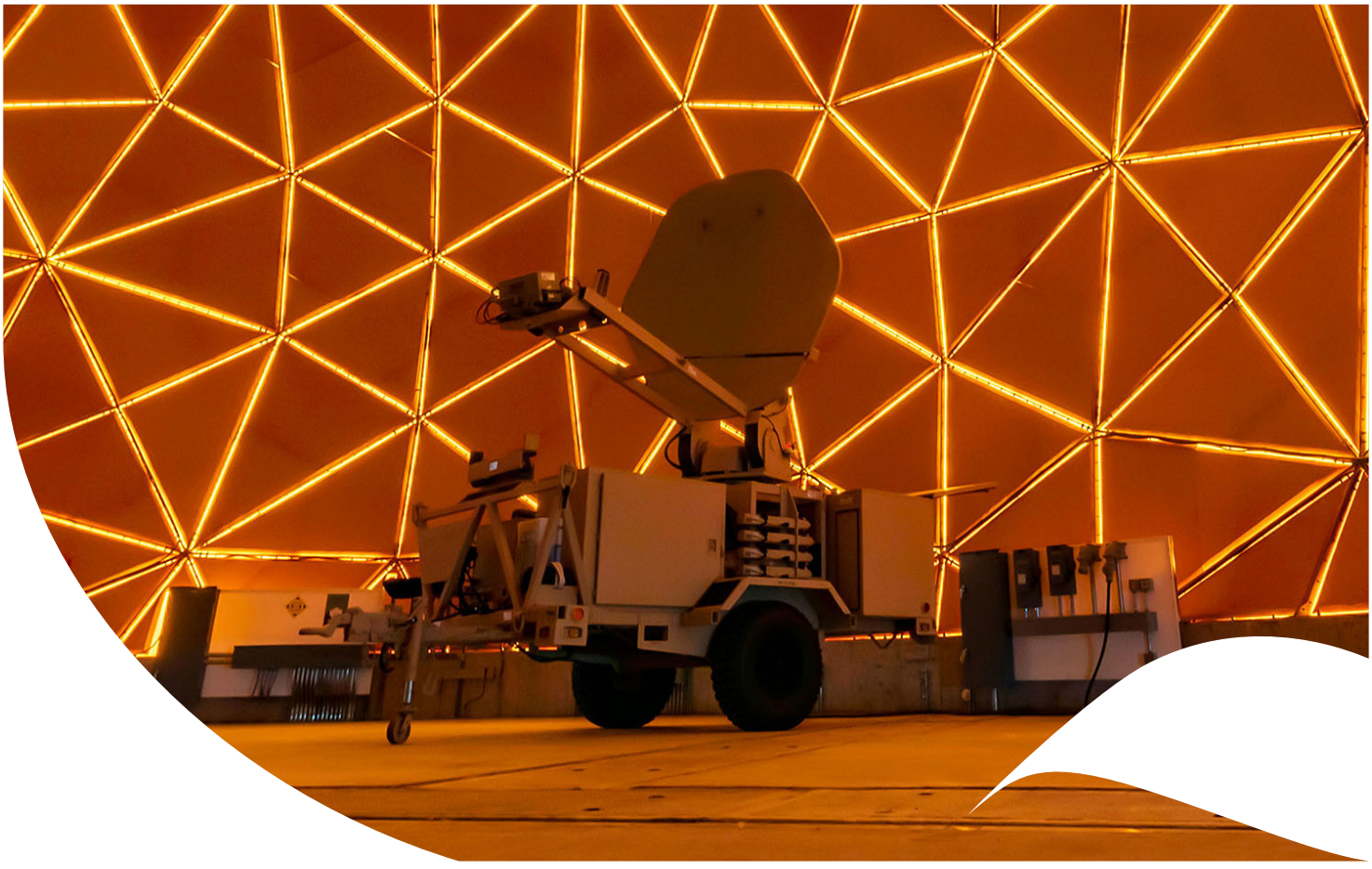
Eve Massingham

The role of the electromagnetic spectrum in all manner of military operations is increasing. The same can be said for all aspects of our everyday civilian lives. Consequently, demand on the spectrum, both for military and civilian purposes is intense. The spectrum, while fully renewable, is not unlimited at any one point in time and allocation of the spectrum for optimum utilisation is key. This policy brief, and the paper it is based on, looks at attempts to use automation technologies to better manage the spectrum while noting the challenges created by signal interference and the dual-use nature of this valuable resource. The work focuses on three issues for the military and its use of the electromagnetic spectrum in light of the increasing use of and demand for the spectrum by both military and civilian users: automation in the management of the spectrum, signal interference, and law of armed conflict implications.

Automation of the spectrum

The idea of automated spectrum management first appeared in International Telecommunication Union (ITU) recommendations in 1992. ITU Recommendation SM.1370-2, containing design guidelines for developing automated spectrum management systems, was issued in 1998 and updated in 2013; it remain in force today. The ITU broadly considers that countries should always seek to automate their spectrum management processes, provided they are properly designed. The optimal automated spectrum system would address not just issues of frequency allocation and channel processing but also licensing, payment, fee and report processing, record keeping, as well as matters such as complaint processing and security.

There is a need for a law and policy rethink in order to best facilitate the use and development of technology to allow automation in the management of the spectrum. In automating



spectrum management, there would be some concern from spectrum licence holders about the preservation of existing spectrum allocations and licences. This needs further legal examination at the domestic level in individual jurisdictions, including investigations about what current domestic legal frameworks may need addressing because they prohibit spectrum monitoring (either intentionally or inadvertently).

Interference

New technologies have the potential to facilitate more harmful military interference in spectrum transmissions — both intentional and unintentional. States retain sovereign rights over their use of the radio frequency spectrum within their own territory. Article 48 of the ITU Constitution makes this particularly clear regarding defence applications. However, Article 45 of the Constitution prohibits harmful interference with others. There is currently little in the way of consequences for failing to comply with the ITU regime. Further, States have demonstrated a reluctance in giving enforcement powers to the ITU. There are formal arbitration and dispute resolution procedures for ITU Member States set out under Articles 41 and 56 of the ITU Constitution but they have not been used by States. The system has been characterised to a large degree by voluntary compliance, and self-interested goodwill and mutual cooperation.

With increasing intentional and harmful interference, there are predictions that a more 'rigid' system may need to evolve in the near future.[1] Ultimately, this could give more options for States seeking a meaningful response to military activities that interfere with their legal rights, but which fall short of a use of force or an internationally wrongful act.

The law of armed conflict

In times of armed conflict, the law of armed conflict (LOAC) seeks to limits the effects of hostilities. There is an overarching principle that attacks shall be directed only against military objectives. However, the spectrum serves both military and civilian purposes. Interference with the spectrum could clearly have significant and potentially life-threatening impacts on civilians, for example if essential services signals were disrupted. But it is not entirely clear whether interference with the spectrum would be covered by the rules relating to attacks and means and methods of warfare.

Even without a clear resolution of the question of whether transmissions over the spectrum, or the frequency range itself, may be considered the objects of attack, three points emerge.

First, under Article 57(1) of Additional Protocol I to the Geneva Conventions ('AP I'), States party to a conflict must exercise constant care to spare the civilian population, civilians and civilian objects. It would be difficult to support an argument that an attack on a military objective, which had the effect of neutralising spectrum frequencies, or denying access to a range of frequencies, which were imperative for civilian health and emergency services, complied with this provision. The constant care provision is therefore of critical import for militaries seeking to use and/or exploit the spectrum.

Second, devices using the spectrum and serving both military and civilian purposes will be subject to the rules prohibiting certain attacks. While military objectives can themselves lawfully be attacked, where they are surrounded by the civilian population and or civilian purpose infrastructure, Article 51(5)(b) of AP I prohibits attacks that would cause disproportionate civilian losses. If it was clear that an attack could be directed only against the part of the device being used by the military, and only at a specific point in time, then it would be lawful. But any broader attack, including one that disabled frequencies for extended periods that may later be needed to serve essential civilian purposes, could be in violation of Article 51 of AP I.

Third, when using the spectrum militaries have an obligation to separate their activities from the civilian population. And this might not always be feasible. For example, Jensen observes that 'at this point, it is not feasible for the United States to segregate its cyber operations from civilian objects and infrastructure as required by Article 58, paragraphs (a) and (b), of [AP I].'[2]

Conclusion

Automated spectrum management has great potential for both civilian and military application. However, States must recall their ITU, LOAC and other international law obligations as outlined above. The incorporation of these obligations into the design of frameworks that give effect to advances in spectrum management and spectrum usage by new technologies is key. Accommodating increasing use of the spectrum in new and different ways, facilitating spectrum monitoring for lawful purposes and protecting the spectrum against not only attack, but also misuse by the military, will be tasks for the legal frameworks going forward. ●

1 Ram S Jakhu, 'Regulatory Process for Communications Satellite Frequency Allocations' in Joseph N Pelton, Scott Madry and Sergio Camacho-Lara (eds), *Handbook of Satellite Applications* (Springer 2017) 359–812.

2 Eric Talbot Jensen, 'War in Cities: Attackers Have Rules to Follow. What About Defenders?' *Humanitarian Law & Policy* (16 March 2017).

Eve Massingham, 'Automation of the Spectrum, Automation and the Spectrum: Legal Challenges when Optimising Spectrum Use for Military Operations' (2021) 3(2) *Law, Technology & Humans* 91–106

This research received funding from the Australian Government's Next Generation Technologies Fund through Trusted Autonomous Systems, a Defence Cooperative Research Centre. The views and opinions expressed are those of the author, and do not necessarily reflect the views of the Australian Government or any other institution. They also do not constitute legal advice. Cover photo by Thomas Robbins / US Army. The appearance of US Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

Law and the Future of War
School of Law
The University of Queensland
law.uq.edu.au/future-war

TRUSTED AUTONOMOUS SYSTEMS DEFENCE CRC

THE UNIVERSITY OF QUEENSLAND AUSTRALIA