Volume **3** (2) 2021 https://doi.org/10.5204/lthj.1854

Automation of the Spectrum, Automation and the Spectrum: Legal Challenges When Optimising Spectrum Use for Military Operations

Eve Massingham[1]
University of Queensland, Australia

Abstract

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 by the military and for civilian purposes, is increasing. 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 is raising a range of issues. Questions arise both because of the role of autonomous capabilities in devices that make use of the spectrum, which have the potential to create demand and interference challenges, and because of the valuable role that autonomous capabilities may play in managing the spectrum itself. This paper looks at attempts to use automation technologies to better utilise and manage the spectrum while noting the challenges created by signal interference and the 'dual-use' nature of this valuable resource.

Keywords: Electromagnetic spectrum; International Telecommunications Union; automation; military operations; interference; international humanitarian law.

Introduction

The electromagnetic spectrum is a highly valuable natural resource.[2] It comprises the range of frequencies, and corresponding wavelengths, of electromagnetic radiation, including all radio waves, microwaves, infrared radiation, visible light, ultraviolet radiation, X-rays and gamma rays.[3] The spectrum is essential to our everyday lives. Its uses range from operating simple everyday tools like garage door openers and baby monitors, to allowing huge advances in medical imaging and treatment.[4] Unsurprisingly, militaries also rely on access to the spectrum for a wide range of activities. In particular, the spectrum plays a central role in all manner of military communication, and therefore in most military operations. Spectrum domination in all military domains—air, land, sea, space and cyberspace—is of interest to many militaries worldwide and the focus of numerous programs.[5] A range of information transmission technological developments, since radiocommunications first changed the nature of warfare following their introduction during the First World War,[6] have brought significant military utility, including the ability to transmit more information, more quickly, at greater distances and more securely. Today, the untethered nature of

[1] The research for this paper received funding from the Australian Government through the Defence Cooperative Research Centre for Trusted Autonomous Systems. The views and opinions expressed in the paper are those of the author, and do not necessarily reflect the views of the Australian Government or any other institution. The author wishes to thank Isabelle Peart for her research work that contributed to this piece and Jason Scholz, Rain Liivoja, Simon McKenzie and Tim McFarland for their feedback on earlier drafts as well as the anonymous reviewers for their comments and suggestions.
[2] The economic value of the spectrum is notoriously difficult to calculate and the International Telecommunications Union (ITU) do not place a figure on it: ITU, Economic Aspects. However, the amount is clearly significant. A report by the Boston Consulting Group estimates that in countries with advanced information and communication technologies, the use of spectrum enabled an increase in Gross Domestic Product of approximately 3.4 per cent between 2010 and 2017: Panhans, "Coming Battle."
[3] Britannica, Electromagnetic Spectrum.
[4] Chan, "Shared Spectrum Access."
[5] Congressional Research Services, Defense Primer, 13, 15.
[6] Britannica, Military Communication.

increasingly autonomous devices means that, for many of them, access is required to the spectrum to effectively communicate (when necessary) with their operating unit (whether that be in the military or civilian context) and with each other.[7] For example, as Wang et al. note, '[a]n efficient, flexible and adaptable spectrum resource sharing method is distinctly important' for swarm technology.[8] Consequently, increasing demands on the spectrum, both for military and civilian purposes, raise concerns about how so many devices can simultaneously make use of the spectrum. These concerns are not new.[9] However, demand, and consequently these concerns, are only increasing as more and more devices make use of the spectrum to function.[10] Efficient utilisation and allocation of the spectrum are key.

As more and more technologies that we use depend on being able to access the necessary parts of the spectrum to function efficiently and effectively, or at all, demand is driving innovation in how to deal with spectrum allocation, spectrum interference and safeguarding of the spectrum for essential purposes. This raises the question of whether new law is needed or whether existing law can adequately be applied to the new developments. While most existing law can be applied to most new technologies most of the time, this will not always be the case.[11] In terms of regulation, Crootof and Ard note two options: the permissive approach for generative or unthreatening technologies (allowing the technological developments to occur without regulatory intervention until some harm is apparent) and the precautionary approach in the case of significant or irreversible threats (placing pre-emptive or proactive restrictions on new technologies).[12] However, regarding the spectrum, the threat of significant or irreversible harm may, in fact, arise from not facilitating new technologies. Emergency services being prevented from having enhanced spectrum access by traditional regulatory limits on spectrum allocation, when the technology itself would allow them to access or make use of a greater range of the spectrum, provides a simple example. In any event, before determining whether new law is needed or existing law can be adapted, the issues that spectrum regulation raise need to be better understood. Ultimately, understanding these relevant legal obligations, and incorporating compliance with them into the design of frameworks that give effect to advances in spectrum management and spectrum usage, will enable advancement in military practice and civilian protection.

This paper focuses on three issues that have already become apparent for the military and its use of the spectrum. Part One focuses on the development of technology to allow automation in the management of the spectrum and the potential need for law and policy rethink to best facilitate this development. Part Two addresses signal interference when using the spectrum (which may occur both unintentionally or intentionally) and the existing legal framework's approach to resolving disputes. Part Three concerns the implications for the spectrum during times of armed conflict. Before turning to look at these issues, this paper provides a brief overview of the spectrum and the overarching legal framework.

What is the Spectrum and How is it Regulated?

The electromagnetic spectrum is the totality of electromagnetic radiation. The spectrum is organised into bands, with different names (e.g., radio waves, microwaves, visible light, ultraviolet radiation) due to their different sources and effects on matter. The frequency and wavelength of the transmission determine, among other things, its geographic reach and the amount of information that can be transmitted. For example, signals travelling at low frequencies can travel a long distance, but only a relatively small amount of information can be transmitted. The extremely high frequency band can only be employed for very short-range transmissions but with the potential for very large amounts of information being transmitted.[13]

Challenges in using the spectrum arise because 'the fact that the spectrum is physically available does not ipso facto mean that it is technically useable'.[14] There are two reasons for this. First, although techniques exist to minimise disturbances within the bandwidth of the transmission—such as the physical orientation of antennas to reduce pickup of unwanted signals[15]—multiple signals at the same frequency at the same point in time may cause interference between the signals and impact effective reception of transmissions.[16] Second, regulation, which currently allocates bands as reserves for specific uses and to specific users typically over long periods (years), is limiting because the spectrum resource is unlikely to be used all of the time or cover

[7] Not all untethered new technologies will rely on continuous spectrum transmission. Some highly autonomous systems are being developed specifically to allow them to operate in communications-denied environments.
[8] Wang, "Machine Learning," 89839–89840.
[9] Levin, writing in 1970, referred to the spectrum as the invisible resource, noting that its full parameters were not in use and technological advances would allow more and more of the spectrum to be used: Levin, Invisible Resource.
[10] Congressional Research Services, Defense Primer; Mountin, "Legality and Implication," 101–107; Jakhu, "Regulatory Process."
[11] Crootof, "Structuring Techlaw," 3, 15.
[12] Crootof, "Structuring Techlaw," 38–46.
[13] See further, Levin, Invisible Resource, 17.
[14] Levin, Invisible Resource, 17.
[15] Mayhan, "Physical Limitations," 639.
[16] See, e.g., US Cybersecurity and Infrastructure Security Agency, Radio Frequency Interference, 2–4.

all of the jurisdiction for which it has been reserved. That is, the current regulatory environment does not allow for signals to use areas of under-utilised spectrum that are reserved for others or make more efficient use of the scarce spectrum resource, nor does it allow off-loading of other possibly congested areas onto free areas of spectrum that would reduce interference and improve communication services.

As such, when multiple users seek to use the same frequency range at the same time, in the same area, this may prevent at least one of the signals from getting through and/or prevent either signal from being received.[17]

A number of methods exist to overcome these challenges. Techniques exist to minimise disruption within a bandwidth—such as the physical orientation and spacing of transmission and reception devices, and frequency and time modulation. Further, technologies that make use of methods such as frequency hopping (jumping signals around) and encoding signals to alter how they travel on the spectrum, are changing the landscape. These technological solutions can overcome the traditional limits of the physical characteristics of the bands within the spectrum such that the spectrum can be more efficiently utilised. However, the use of technological solutions that would allow for more adaptability may require regulatory consideration and ultimately change. The regulatory framework is overseen by the International Telecommunication Union (ITU).

The ITU is an intergovernmental organisation[18] and United Nations (UN) specialised agency.[19] Founded in Paris on 17 May 1865, the role of the ITU was to provide a forum for discussion on the regulation of the telegraph.[20] The overarching legal instruments of the ITU (today) are the *Constitution of the International Telecommunication Union* and the *Convention of the International Telecommunication Union*.[21] As of early 2021, the Constitution and Convention had 191 State parties. The Plenipotentiary Conference 'is the supreme organ of the Union'.[22] It meets every four years and deals with matters based on proposals by Member States and the Council of Member States, which acts on behalf of the Conference.[23] The ITU has three sectors: radiocommunications, standardisation and development.[24] It is the ITU's radiocommunications sector[25] that regulates the global use of the radio frequency spectrum.[26] Its regulatory process is developed at the ITU's World Radiocommunication Conference[27] in the form of ITU Radio Regulations.[28] Central to the framework is the understanding that while national regulatory schemes allocate spectrum usage within their jurisdictions,[29] spectrum allocations within each Member State occur in line with the ITU Radio Regulations Master International Frequency Register[30] and the ITU's spectrum harmonisation (uniform allocation of bands across a region or globally as outlined in the International Radio Regulations Articles, Appendices, Resolutions and Recommendations) system. The ITU reports there are around 200 000 allocations added every year to the currently 2.6 million frequency assignments and that administrations need to ensure compatibility with previous allocations.[31] Regular reviews also occur to ensure consistency with the actual use of the spectrum.[32] This overarching framework and spectrum harmonisation ensure the alignment of spectrum management activities between countries and other international standards bodies, such as the International Civil Aviation Organization, the International Maritime Organization and the World Meteorological Organization. These harmonised systems are particularly critical in densely populated regions where

[17] Levin, Invisible Resource, 17.
[18] ITU, Constitution, art. 2.
[19] See further, Sands, Bowett's Law, ch 3.
[20] ITU, Telegraph Conference.
[21] Adopted in 1992 in Geneva, and as amended by subsequent plenipotentiary conferences. For more information on its development and predecessor documents see ITU, Constitution and ITU, Convention.
[22] ITU, Constitution, art. 7.
[23] ITU, Constitution, art. 8.
[24] ITU, Constitution, art. 7.
[25] Which began in 1906: Sands, Bowett's Law, 106.
[26] ITU, Radio Regulations, art. 8.1.
[27] This body, established under the ITU Constitution, meets every three to four years and has a mandate to revise the Radio Regulations and 'deal with any question of a worldwide character within its competence and related to its agenda': ITU, Constitution, art. 13.
[28] The ITU Radio Regulations complement the Constitutional and Convention and are binding on all Member States: ITU, Constitution, art. 4(3).
[29] For example, in Australia, the *Radiocommunications Act 1992* (Cth) establishes a licensing system where a 'holding' allows access to an allocated part of the spectrum (in line with Australia's ITU obligations) depending on the use and purpose: Department of Communication and the Arts, "Australian Government Held Spectrum Report," 7. In the United Kingdom, it is unlawful to establish, install or use wireless telegraphy stations and/or apparatus without a licence: Wireless Telegraphy Act, 2006, c. 36 (Eng.), s. 8. In Canada, the legislation requires 'authorization' for use of 'distribution undertaking' radio apparatus: Radiocommunications Act, R.S.C. 1985, c. R-2 (Can.), s. 4.
[30] ITU, Convention, art. 12(2)(2)(e).
[31] ITU, Managing the radio-frequency.
[32] ITU, Managing the radio-frequency.

overlapping spectrum use between different States is inevitable[33] and where spectrum must necessarily be reserved for civilian safety purposes.

Part I: Managing the Spectrum: Automating Spectrum Allocation

As noted above, when multiple users seek to use the same frequency at the same time, in the same area, this may prevent the reception of at least one of the signals.[34] However, at the same time, in the same area, there may also be significant unused allocations of other frequencies.[35] This occurs because the current system allocates frequency largely using the traditional model of frequency band allocation. That is, the current regulatory environment does not allow for signals to be 'spread out' to other areas of unused spectrum to reduce interference, even though the technology may allow it. A particular frequency range is allocated in its entirety to a spectrum user. Whether, when and to what extent the holder of an allocation of spectrum makes use of that allocation is up to them. Other users cannot access unused spectrum within that allocation. As such, interference occurs in parts of the spectrum, even though there is significant under-utilisation in other parts of the spectrum. Spectrum management systems are therefore widely acknowledged as being inefficient and not providing optimal use of the spectrum. Improved spectrum management is needed to reduce instances of signal interference and allow for unused spectrum to be utilised. This is something that can be improved manually. However, the role that automation could play is significant.

Technological solutions are now also making it possible for more transmissions to be sent at any one point in time in the same geographic area. Increasing the usage of multiple frequency channels within a band of the spectrum is one example of such technological development.[36] Further, new technologies are developing that can identify under-utilised spectrum, thus facilitating a different approach to spectrum usage. Bluetooth technology, for example, employs 'frequency hopping' techniques that allow devices to operate across different frequencies based on availability and, therefore, share the available spectrum most efficiently.[37] These technologies are significant breakthroughs, but the challenges of managing the spectrum for optimal utilisation remain.[38]

However, the quest to do things differently in relation to allocation and use of the spectrum is clearly on—both in the civilian and military contexts. Dynamically assigning and trading the spectrum as needed, rather than having static allocated spectrum sit unused, is the focus of some considerable attention. Telecommunications companies, who have licences over certain parts of the spectrum, have become increasingly efficient at managing their allocation of the spectrum—principally because it is economically valuable for them to do so. The United States (US) military is, unsurprisingly, particularly invested in spectrum automation. The task of using artificial intelligence to allow 'autonomous radios collectively sharing wireless spectrum to transmit far more data than would be possible by assigning exclusive frequency to each radio'[39] has been the subject of various Defense Advanced Research Projects Agency (DARPA) projects and the recent DARPA Spectrum Collaboration Challenge that concluded in October 2019.[40] However, the US is not alone in pursuing this research. For example, in Australia, a project of the Trusted Autonomous Systems Defence Cooperative Research Council (the funder of this research) is the Distributed aUtonomous Spectrum managemenT (DUST) project, which is led by Consunet Pty Ltd with RMIT University, the University of Melbourne, the University of Sydney, and Defence Science and Technology Group. 'DUST aims to research, develop and demonstrate near real-time autonomous spectrum management to deliver orders of magnitude increase in agility and efficiency cost savings for Australian Defence and commerce'.[41] A number of companies also offer commercial automated spectrum management services. Progira, a Swedish company, for example, offers tailored and integrated spectrum management systems, which include interference analysis and spectrum monitoring.[42] LS Telecom, based in Germany, similarly advertise spectrum monitoring services.[43] Wrap International[44] and TCI[45] are further examples.

[33] For example, in Europe, the European Commission Radio Spectrum Committee implements the Radio Spectrum Policy: Department of Communication and the Arts, Australian Government Held Spectrum Report.
[34] Levin, Invisible Resource, 17.
[35] Levin, Invisible Resource, 17.
[36] Couture, "New Weapons."
[37] Tilghmann, "AI Will Rule the Airwaves," 30, 33. See also Pandit, "An Overview."
[38] Couture, "New Weapons."
[39] Tilghmann, "AI Will Rule the Airwaves," 30.
[40] Koziol, "DAPRA's Grand Challenge".
[41] Trusted Autonomous Systems Defence CRC, Projects.
[42] Progira, Spectrum Management.
[43] LS Telcom, Smart Solutions.
[44] Wrap International, Spectrum Management.
[45] TCI, Spectrum Management.

The ITU is in fact the driving force behind much of this work. Automated spectrum management first formally appeared in ITU recommendations in 1992. As demand for radio services increased, 'enabling more efficient utilization of the spectrum' was highlighted.[46] Recommendations that, for example, 'administrations which intend to procure new spectrum management and monitoring systems should consider procuring an integrated, automated system using a common relational database'[47] and '[a]dministrations should be encouraged to undertake the use and further development of such equipment'[48] followed somewhat regularly thereafter in the ITU Radiocommunication Assembly documentation. The ITU recommendations issued in 2013 on the design of guidelines for developing automated spectrum management systems remain in force today.[49] The ITU broadly considers that countries should always seek to automate their spectrum management processes, provided the spectrum management systems are properly designed.[50] The optimal automated spectrum system would not only address issues of frequency allocation and channel processing, but also licensing, payment and fee and report processing, report keeping, and matters such as complaint processing and security, making it a very comprehensive system.[51]

In automating spectrum management, there would be some concern about changes to the long-established status quo and interest from some spectrum licence holders in the preservation of existing spectrum allocations and licences. Providing certainty to licence holders in allowing them to retain existing spectrum holdings, as well as opportunities to acquire new capacity, will be key.[52] This may need further legal examination at the domestic level in individual jurisdictions.[53] However, before automated spectrum management becomes a tangible and viable reality impacting the need for potential new domestic laws, existing legal frameworks in various jurisdictions may need some reconsideration—in so far as they limit efforts to automate spectrum management in the first place. These limitations arise because automating spectrum management necessarily requires monitoring the use of the spectrum. This may fall foul of domestic laws prohibiting such conduct for very valid policy reasons such as protecting privacy and national security. Defence has particularly significant allocations of spectrum, but also has particularly high needs at particular times—for example, during military exercises and operations. For example, as far back as 15 years, a report on military radio-frequency allocations noted that '[p]ressure is being brought to bear on government agencies to make military spectrum available for commercial development in the interests of advancing public benefit'.[54] If these spectrum allocations are handed over to civilian users, 'military radio based systems may be required to relocate to other parts of the spectrum or to be prematurely withdrawn from service'.[55] This may have impacts for national defence and security. These consequences may be avoidable to some degree with better spectrum management.

In Australia, for example, the *Telecommunications (Interception and Access) Act 1979* (Cth) provides that it is prohibited to intercept a 'communication passing over a telecommunications system'.[56] Does this apply to monitoring the spectrum? Is monitoring the spectrum an 'interception' of a 'communication passing over a telecommunications system'? If so, is there a relevant exemption? A telecommunications service is specifically not 'a service for carrying communications solely by means of radiocommunication',[57] indicating that not all communications over the spectrum would be covered by the Act. However, for those that are, 'interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication'.[58] Communication is defined to include the data pertaining to the conversation or message[59] and specifically includes where a person 'makes use of' a record obtained by an interception.[60] This means that monitoring communications that are part of the telecommunications system over the spectrum could be illegal because even without recording the speech or images, for example, the data about when, where, and for how long the communication took place could fall within the prohibition. There are exemptions to these rules, for example, for the Australian Security Intelligence

[46] ITU Radiocommunication Assembly, Recommendation 182–4
[47] ITU Radiocommunication Assembly, Recommendation ITU-R SM 1537, recommendation 1.
[48] ITU Radiocommunication Assembly, Recommendation ITU-R SM.182–5.
[49] Radiocommunication Sector of ITU, Design Guidelines.
[50] Radiocommunication Sector of ITU, Handbook, 2.
[51] Radiocommunication Sector of ITU, Handbook, 3–5.
[52] Deloitte, Mobile Nation, 19.
[53] See, e.g., Selvadurai, Enhancing the Effectiveness, 307–308.
[54] Combined Communications Electronics Board (CCEB), Policy for the Coordination, para 410. The CCEB is a five-nation (Australia, Canada, New Zealand, the US and the United Kingdom) military communication and electronic systems forum that coordinates any military communication and electronic systems matter referred to it by member nation States.
[55] CCEB, Policy for the Coordination, para. 410.
[56] *Telecommunications (Interception and Access) Act 1979* (Cth) (Aust.) s 7.
[57] *Telecommunications (Interception and Access) Act 1979* (Cth) (Aust.) s. 5.
[58] *Telecommunications (Interception and Access) Act 1979* (Cth) (Aust.) s. 6.
[59] *Telecommunications (Interception and Access) Act 1979* (Cth) (Aust.) s. 5.
[60] *Telecommunications (Interception and Access) Act 1979* (Cth) (Aust.) s 5A.

Organisation to monitor communications and for some criminal proceedings; however, management of the spectrum is not the basis of one of these exemptions.[61]

In New Zealand, the Defence Force is generally exempt from the prohibition on interception of radiocommunications. This is the case when acting in the defence of New Zealand;[62] for the protection of the interests of New Zealand;[63] when contributing forces under collective security treaties, agreements, or arrangements;[64] and when contributing forces in accordance with the principles of the UN Charter.[65] Monitoring the spectrum in peacetime to allow for automation of the spectrum for Defence purposes could constitute the protection of the interests of New Zealand.

Coming from jurisdictions that have clearly given regard to tensions between privacy and national security interests, these two examples highlight the challenges in making automated spectrum management become a tangible and viable reality. A policy decision could be made to allow certain actors to monitor the spectrum for the purposes of both the research necessary to design and implement autonomous spectrum management, as well as for the ongoing management of the spectrum, and this could then be included in the legal framework by way of exemptions from liability for interception offences. This may be needed for Defence to ultimately make the best use of the spectrum in national security and defence interests. While the better manual allocation of the spectrum would likely have many benefits itself, the efficiencies of automation would allow this to happen with greater speed, and therefore efficiency. However, any such change would need to be considered in light of any constitutional or human rights law implications.

Part II: Use of the Spectrum: Interference

Interference is '[t]he effect of unwanted energy due to one or a combination of emissions, radiations, or inductions … in a radiocommunication system, manifested by any performance degradation'.[66] In simpler terms, as noted above, when multiple users seek to occupy the same frequency at the same time, in the same area, this could impair the reception of at least one of the signals. New technologies have the potential to facilitate more harmful military interference (e.g., jamming, which 'involves overloading targeted radio frequencies with so much electronic noise that communications cannot get through to their intended destinations').[67] However, as Kaplan notes, causing spectrum interference that affects the military can also be unintended[68] and very simple. Increasing demand for the spectrum has the potential to create more unintentional interference. This is likely to sometimes be the case even with the use of increasingly sophisticated automated spectrum management systems, simply due to the sheer volume of demand.

In the military context, intentional interference can be very serious. Indeed, intentional use of signal interference by and against the military is a military strategy.[69] Mountin, writing about satellites, discusses that at the most serious end, signal interference could, in fact, amount to an armed attack within the meaning of Article 51 of the UN Charter, invoking the right to use force in self-defence. She uses the example of disrupting satellite communications to intentionally cause the collision of two commercial airliners over a heavily populated city causing measurable life and property loss.[70] Measures falling short of an armed attack may also invoke other international law remedies such as restitution and compensation,[71] and within the framework of the ITU, as is discussed further below. Myres et al. note that States may be held responsible for failing to contain and constrain jamming activities under international law, and 'States directly menaced [by jamming] can reasonably be expected to take measures against such threats wherever they occur'.[72]

[61] *Telecommunications (Interception and Access) Act 1979* (Cth) (Aust.) s 5B.
[62] *Defence Act 1990* (New Zealand) s 5(a).
[63] *Defence Act 1990* (New Zealand) s 5(b).
[64] *Defence Act 1990* (New Zealand) s 5(c).
[65] *Defence Act 1990* (New Zealand) s 5(d).
[66] ITU, Radio Regulations, reg 1.166. There are three types of interference set out under the Radio Regulations: permissible interference, which is predicted and complies with the international framework; accepted interference, which is of a higher level than permissible interference but 'has been agreed upon between two or more administrations without prejudice to other administrations'; and harmful interference, which 'endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service': ITU, Radio Regulations, reg. 1.167–9.
[67] Savage, Politics of International Telecommunications, 436.
[68] Mountin, "Legality and Implications," 104, 131.
[69] US Department of Defense, Electromagnetic Spectrum.
[70] Mountin, "Legality and Implications," 177.
[71] See, e.g., Responsibility of States, arts 31–36.
[72] McDougal, Law and Public Order, 284.

States retain sovereign rights over their use of the radio frequency spectrum within their territory.[73] Article 48 of the *Constitution of the International Telecommunication Union* makes this particularly clear regarding Defence applications. Article 48(1) provides that 'Member States retain their entire freedom with regard to military radio installations' (although Article 48(2) does require that 'so far as possible' military radio installations observe the provisions—in particular, in relation to giving assistance in case of distress and the measures to prevent harmful interference). The meaning of Article 48 has been the subject of some consideration by World Radiocommunication Conferences to clarify that Article 48 does not refer to stations used for general government purposes—only military purposes—and that 'installations' has a broad meaning to include frequency allocations and satellites.[74] Further, State practice supports this understanding.[75] This means that militaries are not generally subject to ITU provisions.[76] However, while defence forces tend to be exempted from many of the ITU and domestic legal frameworks to regulate the spectrum, defence force operations clearly do not exist in a spectrum vacuum. The ITU system could be a suitable forum for States to resolve international disputes regarding interference that impacts defence and does not constitute force or an internationally wrongful act.

Not only do defence force operations take place while 'competing' for spectrum access with civilians, but spectrum regulation and harmonisation among military allies remain key to the prevention of unintentional signal inference. A five-nation Combined Communications-Electronics Board (CCEB) (Australia, Canada, New Zealand, the US and the United Kingdom) coordinate any military communication and electronic systems matter referred by a member nation. The national frequency managers of the CCEB countries meet, usually every year, to develop and establish combined radio-frequency management policies and procedures and seek a common approach to items raised at the World Radiocommunications Conference.[77] Similarly, the Consultation, Command and Control Board of the North Atlantic Treaty Organization (NATO) Standardization Office is responsible for setting policies on spectrum management for national and NATO military operations. NATO identifies its 'overarching goal' for spectrum management as being 'to provide free use of the spectrum for operational forces or peacetime organisations'.[78] NATO's approach to standardisation and harmonisation rests on three pillars: '[i]nteroperability between all spectrum management actors at all levels: single services, national and a coalition'; 'maintenance of a central data repository of frequency-related information accessible by all actors all levels'; and 'respect of ITU and national radio regulations'.[79] These bodies play a key role in spectrum regulation and harmonisation among military allies.

However, the reality, of course, is that standardisation and harmonisation, even with advances in automation of spectrum management, is not a complete answer, and interference will continue to be an issue. Article 45 of the *Constitution of the International Telecommunication Union* prohibits harmful interference providing that 'Each Member State undertakes to require the operating agencies which it recognizes and the other operating agencies duly authorized for this purpose to observe the provisions' and 'recognize[s] the necessity of taking all practicable steps to prevent the operation of electrical apparatus and installations of all kinds from causing harmful interference'.[80] The application of Article 45 is required to be exercised with 'the utmost good will and mutual assistance',[81] however responsibility ultimately lies with the administration of the country that has jurisdiction over the place of interference. Where an administration becomes aware that one of its stations is causing harmful interference, it is required to take the necessary steps to eliminate such interference.[82] Given the focus on automated spectrum management in Part One, it is relevant to note here that whether the interference is a result of a manual or automated process does not appear to be a relevant consideration. The administration's obligation is related to the outcome—harmful interference—not the cause of it.

[73] ITU, Constitution, preamble.
[74] Jeanty, Radio Regulations Board.
[75] For example, Mexico brought up a State's ability to regulate the use of the radiofrequency spectrum in their own territory in a case before the World Trade Organization: *Mexico – Measures Affecting Telecommunications Services*, Panel Report, WT/DS204/R (2 April 2004), para 4.88; In a dispute about the annulment of an agreement for lease of a particular band of the electromagnetic spectrum on two satellites, India attempted to justify its termination on the grounds of an 'essential security interest' given its decision to reserve this band of the spectrum for military applications: *Deutsche Telekom AG v Republic of India* (Interim Award), PCA Case No. 2014–20 at paras. 183, 371, cf. para. 221.
[76] See also that States have domesticated this exemption found in art. 48 of the Constitution of the ITU: e.g., in Australia, the relevant law does not apply to acts or omissions by Defence members 'the purpose of which relates to … research for purposes connected with defence [or] intelligence': *Radiocommunications Act 1992* Cth (Aust.), art. 24; See also, *Wireless Telegraphy Act 2006* c. 36 (Eng.); Ofcom, Spectrum Framework Review, para. 3.9; *Title 47 Telecommunications (1943), U.S.C.* § 302a(c).
[77] Australian Defence Force, Communication and Information Systems.
[78] NATO Standardization Office, Spectrum Management Allied Data, para. 2.1
[79] NATO Standardization Office, Spectrum Management Allied Data, para. 2.1
[80] ITU, Constitution, arts. 45(2)–(3).
[81] ITU, Radio Regulations, reg. 15.22.
[82] ITU, Radio Regulations, regs.15.34, 15.37.

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.[83] The ITU has made comment on interference issues. For instance, in Resolution 173 of the Plenipotentiary Conference of the ITU (Guadalajara, 2010), the ITU Conference condemned Israel's ongoing interference with and interruption to Lebanon's telecommunication facilities.[84] Despite this, the conference only instructed that the cessation of violations be monitored and that there be a report back to the Council. No stronger action appeared to be taken against Israel.[85] There are formal arbitration and dispute resolution procedures for ITU Member States set out under Articles 41 and 56 of the ITU Constitution. Article 56 provides that disputes are to be settled 'by negotiation, through diplomatic channels, or according to procedures established by bilateral or multilateral treaties concluded between them for the settlement of international disputes.' If no settlement can be achieved, Article 41 of the ITU Convention makes an arbitration procedure open to the disputing Member States. Interestingly, the arbitration option provided for in Article 41 of the ITU Convention, and the dispute resolution process provided for in Article 58 of the ITU Convention, have not been used by States.[86]

The ITU has traditionally been very effective in its task of arriving at international agreement for the management of the spectrum. Commentators have reflected on why this is so. Alvarez, writing about international organisations as lawmakers, notes the socialising impact of international organisations with technical rule-making mandates. He notes their engagement in 'continuous forms of regulation', often of a less controversial nature[87] than much of international law, means that they are able to effectively serve their intended purpose. The ITU's ability to set and meet '[g]reat expectations' of the international community in solving problems and finding 'solutions paving the way for further improvement and efficiency in radio-frequency management' has been lauded.[88] As Mountin observes, voluntary compliance, and indeed, self-interest, has meant that 'goodwill and mutual cooperation' has, in the past, been able to ensure that most spectrum interference issues have been able to be resolved.[89] However, this 'mutual cooperation' may be coming to an end. Mountin notes that the lack of compulsory dispute resolution mechanisms within the ITU means that intentional and harmful interference with frequencies is increasing, and yet States are not acknowledging this.[90] Jakhu predicts that 'more rigid and extensive international regulations and procedures [are likely] in the not too distant future'.[91] Ultimately, this could give more options for States seeking a meaningful response to military activities that interfere with their legal rights but fall short of a use of force or internationally wrongful act.

Because the spectrum is such a valuable resource for military operations, key components of military spectrum work include protection against offensive spectrum interference operations by adversaries as well as using the spectrum to disrupt the operations of the adversary. Militaries are investing in a variety of technologies. For example, the Royal Australian Air Force EA-18G Growler is described as 'an electronic attack aircraft … capable of disrupting, deceiving or denying a broad range of military electronic systems, including radars and communications.'[92] The potential for the use of these technologies may engender further international discussion regarding interference rules and require consideration of legal frameworks regarding noninterference with another State's affairs. The implications of these devices and their potential impact on the civilian population and infrastructure in times of armed conflict will be discussed below.

Part III: Military Attacks and the Spectrum: Questions for International Humanitarian Law

In times of armed conflict, international humanitarian law (IHL) seeks to limit the effects of armed conflict. The principal documents of IHL, the Geneva Conventions of 1949 and their Additional Protocols of 1977, set out a number of principles for the conduct of armed conflict specifically aimed at protecting those not, or no longer, taking part in hostilities. An overarching principle in IHL is that attacks shall be directed only against military objectives.[93] Military objectives are those 'objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage'.[94] Additionally, and more specifically, attacks on 'objects indispensable to the survival of the civilian population' are prohibited,[95] as are methods or

[83] Mountin, "Legality and Implications," 122.
[84] ITU, Resolution 173 (Guadalajara, 2010), 692.
[85] ITU, Landmark Decisions.
[86] Mountin, "Legality and Implications," 135.
[87] Alvarez, International Organisations, 218.
[88] Noll, "ITU in the 21st Century," 64; Roberts, "Lost Connection," 1118.
[89] Mountin, "Legality and Implications," 135.
[90] Mountin, "Legality and Implications," 135–136.
[91] Jakhu, "Regulatory Process,"3.
[92] Royal Australian Air Force, EA-18G Growler.
[93] Protocol Additional to the Geneva Conventions (API), art. 48; Henckaerts, Customary International Humanitarian Law, vol. 1, rule 1.
[94] API, art. 52(2); Henckaerts, Customary International Humanitarian Law, vol. 1, rule 8.
[95] API, art 54.

means of warfare that may 'damage the natural environment and thereby … prejudice the health or survival of the population'.[96] As we have seen, the spectrum serves both military and civilian purposes. While interference with the spectrum could clearly have significant and potentially life-threatening impacts on civilians if essential services signals were disrupted, it is not necessarily clear that interference with the spectrum—to the extent that it is not in the physical domain—would be covered by IHL rules relating to attacks and the means and methods of warfare.

McCormack notes the 'implied tangibility' and 'physical materiality' in the meaning of both civilian objects and military objectives,[97] thus raising the question of whether the spectrum could be classified as an object capable of attack. In the cyber context, the majority of experts in the Tallinn Manual 2.0 process have concluded that physical destruction is required for something to be a military objective.[98] However, it should also be noted that Rule 101 states that '[c]yber infrastructure [which includes both physical and virtual systems[99]] used for both civilian and military purposes is a military objective'.[100] The incapacitation of a virtual system could arguably take place without lasting physical damage to the system. Further, the majority accept that a 'cyber operation targeting data may sometimes qualify as an attack when the operation affects the functionality of cyberinfrastructure or results in other consequences that would qualify the cyber operation in question as an attack'.[101] This suggests that there remains a number of unanswered questions here. Liivoja and McCormack have critiqued the requirement of tangibility to be the object of an attack covered by IHL. They see this approach as not fully appreciating the value that could be obtained by destroying data.[102] Gisel, Rodenhauser and Dormann have also recently observed that 'the obligations to respect and protect medical facilities … must be understood and extending to medical data belonging to those facilities.'[103]

In any event, even without a clear resolution of whether transmissions over the spectrum or the frequency range itself can be considered the objects of attack under IHL, three points are clear. First, the obligation in Article 57(1) of Additional Protocol I to exercise constant care remains. Second, devices using the spectrum, and the spectrum to the extent that it is a physical object, serving both military and civilian purposes, will be subject to the IHL rules prohibiting certain attacks. Third, when using the spectrum, militaries have an obligation to separate their activities from the civilian populations. These will now be discussed.

Constant Care

Article 57(1) of Additional Protocol I requires that '[i]n the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.' This principle is recognised in customary IHL,[104] and indeed the commentary to this provision notes that it supplements the obligation to distinguish between the military and civilian population.[105] The commentary further notes that 'the term "military operations" should be understood to mean any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat', arguably making it a much broader concept than an 'attack' which requires an evident physical consequence.[106] Thus, in addition to the prohibitions on certain attacks, the conduct of military operations must have regard to civilian needs. It would be difficult to support an argument that an operation against a military objective, which had the effect of neutralising spectrum frequencies or denying access to a range of frequencies and were imperative for civilian health and emergency services, was lawful in compliance with Article 57(1*)*. The constant care provision is therefore of critical import for militaries seeking to use and/or exploit the spectrum.

The Legality of Attacks on Objects Using the Spectrum During Armed Conflict

Although it is absolutely fundamental to IHL that 'the Parties to the conflict … at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly … direct their operations only against military objectives',[107] the reality of this distinction is not always clear cut. It has been noted that 'as a matter of law, status as a civilian object and military objective cannot coexist; an object is either one or the other'.[108] However, as Dinstein

[96] API, art 55.
[97] McCormack, International Law, 225.
[98] Schmitt, Tallinn Manual, 437. And see, e.g., Schmitt, "Wired Warfare", 342.
[99] Schmitt, Tallinn Manual, glossary 'cyber infrastructure'.
[100] Schmitt, Tallinn Manual, rule 101.
[101] Schmitt, Tallinn Manual, 437.
[102] Liivoja, "Virtual Battlespace*"*, 52–53.
[103] Gisel, "Twenty Years On", 31.
[104] Henckaerts, Customary International Humanitarian Law, vol. 1, rule 15.
[105] Sandoz et al, Commentary, 680.
[106] Sandoz et al, Commentary, 680.
[107] API, art. 48; Henckaerts, Customary International Humanitarian Law, vol. 1, rule 1.
[108] Schmitt, Tallinn Manual, 445.

observes, 'some intermingling of civilians/civilian objects with combatants/military objectives is virtually inevitable'.[109] In addition to ordinarily civilian objects being able (through their location, purpose or use) to become military objectives, and the reality of urban sprawl surrounding military objectives with civilian objects, it is evident that some objects—particularly key pieces of infrastructure—have important and, in some cases, vital use by both the military and the civilian population. Jensen, writing in 2010, notes the reality of almost all US Government communications, including classified communications, using 'civilian lines of communication' and a 'near-complete reliance on commercially produced civilian hardware and software'.[110] Indeed, it is often the case that civilian and military users share infrastructure.[111]

The use of an object for a military purpose, although making it a military objective (and not a civilian object), 'does not exclude the possibility of simultaneous civilian use'.[112] To again take the cyber analogy, the findings in Tallinn Manual 2.0 assert that 'there is no reason to treat computer networks differently' in terms of their 'dual-use' nature than you would a road that was used by both military and civilians.[113] Road networks, electricity networks and some fuel depots are classic examples that illustrate the dual-use point. During the Second Gulf War, coalition forces targeted the Iraqi electrical grid. This attack crippled the command and control systems of the Iraqi military. However, it also disrupted the operation of water purification and sewage treatment plants. This resulted in epidemics (including cholera and typhoid), led to an estimated 100 000 deaths and doubled the infant mortality rate.[114]

As such, even if you have a military objective in the device that is making use of the spectrum, whether it would actually be feasible to target this device only, without violating other rules of IHL, would very much depend on the circumstances. While military objectives can themselves lawfully be attacked, where they are surrounded by the civilian population and or civilian purpose infrastructure, IHL prohibits attacks that:

> may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[115]

As was pointed out in the Tallinn Manual:

> [a]ny damage, destruction, injury, or death resulting from disruption of [essential civilian services such as emergency response, civil defence, disaster relief, law enforcement, medical records and diagnosis etc] would have to be considered in determining whether a prospective attack on the [in that case, Internet] comports with the rule of proportionality.[116]

Mountin also makes this same analysis regarding limitations on attacks against dual-use objects in relation to satellite systems.[117] If it were 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 Additional Protocol I.

Finally, the result of finding that cyberinfrastructure is a potential military objective is not that the whole of the internet is to be treated as a military objective.[118] 'The International Group of Experts agreed that, as a legal and practical matter, virtually any attack against the Internet would have to be limited to discrete segments thereof'.[119] Arguably, the same principle would apply in relation to a device using the spectrum. A device transmitting for the military over the electromagnetic spectrum could, therefore, lawfully be the target of, for example, a disruptive signal attack or jamming episode that made part of the transmitting device unusable for military operations.

[109] Dinstein, Conduct of Hostilities, 174.
[110] Jensen, Cyber Warfare, 1535.
[111] See, Schmitt, Tallinn Manual, 445.
[112] Harvard Program on Humanitarian Policy and Conflict, *Commentary*, 119.
[113] Schmitt, Tallinn Manual, 446.
[114] Rizer, "Bombing Dual Use Targets."
[115] See API, art. 51(5)(b).
[116] Schmitt, Tallinn Manual, 447.
[117] Mountin, "Legality and Implications," 157–166.
[118] Schmitt, Tallinn Manual, 446.
[119] Schmitt, Tallinn Manual, 446.

The Legality of Using the Spectrum During Armed Conflict

The key focus in IHL, and indeed international criminal law, is primarily on the attacker. In discussing precautions in air and missile warfare, it is observed that '[c]ustomary law and treaties clearly do not impose obligations on the defender comparable to those of a belligerent launching an attack'.[120] However, it is not only the actions of the attacking party that are relevant. The party using the spectrum also needs to have regard to IHL. Parties to the conflict have obligations under Article 58 of Additional Protocol I:

> …to the maximum extent feasible:
>
> endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives;
> avoid locating military objectives within or near densely populated areas;
> take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations.

The International Criminal Tribunal for Former Yugoslavia (ICTY) has found that these are principles of customary IHL that appear 'not [to be] contested by any State'.[121] The Eritrea–Ethiopia Claims Commissions has held similarly.[122] However, Dinstein notes that 'commentators tend to view them more as recommendations than strict obligations',[123] and Sassòli and Quintin characterise the ICTY's view on the customary IHL status of Article 58 as 'astonishing' given the lack of State acceptance for rules imposing the same obligations on the defender as the attacker.[124] Sassòli and Quintin observe that during the negotiation of Additional Protocol I, several States made it clear that Article 58 did not impact their abilities to organise their national defence, and that the obligation to take 'feasible' precautions 'must be understood as taking … military considerations into account'.[125] Nonetheless, Jensen,[126] in particular, has drawn attention to the obligations on States under Article 58 'to the maximum extent feasible' 'to endeavour' to keep military objectives and civilian objects separate and 'to take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations'.[127] Jensen points out the stark disparity between the liability of an attacker who violates IHL (potentially liable as a war criminal for a grave breach of the Geneva Conventions) and a defender who does so (no individual criminal liability), even though it is the defender 'who is in the best position to protect civilians'.[128]

> It is the defender who is in the best position to know the placement and condition of the local civilians. The defender is more able than the attacker to know and control movements of the population when under attack from forces outside urban areas. The defender can most easily channel civilians into places of safety or away from anticipated areas of hostile activities. It is the defender who determines the proximate position of military objectives to civilians within urban areas.[129]

With those devices using the spectrum that have both military and civilian purposes, it is even more important that States take those measures necessary to separate the civilian and military domains. 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 Additional Protocol I to the 1949 Geneva Conventions'.[130]

Blurring the lines between the two can have significant humanitarian consequences for populations if their own governments co-locate vital civilian services and infrastructure with military assets that constitute legitimate military objectives. Automation of spectrum management, for all its other benefits, may actually make this separation even more difficult if dynamic allocation is allowed between military and civilian uses. As we have seen above, bandwidth of the spectrum is specifically allocated to a range of purpose, including general civilian use, emergency services use and military use. This presents a potentially problematic combination in times of armed conflict. Further, the increasing demand on the spectrum outlined earlier in the paper will mean that even within military spectrum allocations—and indeed for the military in seeking additional spectrum

[120] Sassòli, "Active and Passive Precautions."
[121] *Prosecutor v Kupreskić*, Judgment, IT-95-16-T, para. 524.
[122] Eritrea–Ethiopia Claims Commission, Partial Award at 417, 425.
[123] Dinstein, Conduct of Hostilities, 173.
[124] Sassòli, "Active and Passive Precautions."
[125] Sassòli, "Active and Passive Precautions," 117.
[126] Jensen, Cyber Warfare. See also Jensen, War in Cities.
[127] Protocol Additional to the Geneva Conventions, art. 58(c).
[128] Jensen, War in Cities.
[129] Jensen, War in Cities.
[130] Jensen, War in Cities.

allocation for military operations—there will be a need to negotiate with civilian parties and national administrators to access spectrum that is being used by both civilian and military entities.[131]

On a more positive note, Jensen observes that 'the emergence of advancing technology provides a mechanism for defenders to more easily and more fully comply with their obligations to segregate or protect the civilian population'.[132] The Geneva Conventions and their Additional Protocols make no specific reference to autonomy in military operations. There is only very limited reference in other specific regulations applicable in times of war addressing this topic. For example, automation caused concern in the early regulation of weapons of war, with projectiles deployed from uncrewed balloons set to a timer being quickly addressed by the international community with a prohibition.[133] The 'discharge of projectiles from balloons' was banned at the First International Peace Conference in 1899 in The Hague (although the ban was initially for a five-year period, it was then extended in 1907 and technically remains binding).[134] The use of similar weapons, in urban environments and not allowing for oversight of the target, would also be in violation of IHL.[135] In contrast, The Hague Convention VIII Relative to the Laying of Automatic Submarine Contact Mines of October 18, 1907, is an early example of how automation may be compatible with military operations.[136]

The obligations under IHL are to limit the effects of armed conflict—there is no obligation to eliminate them. Further, the law does not require the deployment of any specific weapon or tactic in any particular circumstance, even if it has better humanitarian outcomes. As long as the weapon used complies with the law, it does not matter if it is not the one that causes the least suffering. This means that there would be no legal obligation under IHL to use autonomy even where it delivered better IHL compliance.[137] That said, autonomy may deliver significant benefits from a military perspective. As such, any autonomous system—including a spectrum management one—that allows for a greater exercise of care in attacks could deliver benefits in terms of civilian protection, provided it does not also jeopardise the separation of military and civilian required by the defender under the laws of war.

Conclusion

The electromagnetic spectrum is facing huge demands, and the current regulatory system does not provide for optimum utilisation, nor does it provide for consequences for creating harmful interference. However, just as technology is creating a problem, it is solving one too. Automated distribution of the spectrum to allow for better spectrum management has great potential for civilian and military applications. It is already being harnessed, to some extent, including by commercial spectrum users. As we move towards both greater demand on the spectrum—through new technologies drawing on the spectrum, and greater capacity of the spectrum through new ways of using and monitoring it—States must recall their ITU, IHL and other international law obligations mentioned throughout this paper. 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. Arguably, at least in some jurisdictions, optimal utilisation of technological developments will require legislative and/or policy change. Accommodating increasing use of the spectrum in new and different ways, facilitating spectrum monitoring for lawful purposes, and protecting the spectrum against attack and misuse by the military will be tasks for the legal frameworks going forward. Optimal usage of the spectrum will benefit warfighters, but only where it also benefits civilians will it have the potential to be an effective tool for the military to achieve their objectives.

[131] CCEB, Policy for the Coordination, para. 4.12.
[132] Jensen, War in Cities.
[133] Massingham, "Radio Silence."
[134] Declaration (IV,1), to Prohibit. The 1907 declaration was due to expire at the close of this projected Third Peace Conference, scheduled for 1914 and delayed due to the outbreak of the First World War. No Third Peace Conference has ever taken place.
[135] API, arts 48 and 51(5); Henckaerts, *Customary International Humanitarian Law*, vol 1, rule 1.
[136] Liivoja, "Autonomous Weapons?"
[137] Law and the Future of War Research Group, Submission to the ADF.

Bibliography

Primary Sources

Australian Defence Force. "Communication and Information Systems Series." Australian Defence Doctrine Publication 6.0. Last modified June 2012. https://www.defence.gov.au/adfwc/Documents/DoctrineLibrary/ADDP/ADDP_6-0_CIS.pdf

Combined Communications Electronics Board. "Policy for the Coordination of Military Radio Frequency Allocations and Assignments Between Cooperating Nations." April 2005. https://www.dau.edu/cop/e3/DAU%20Sponsored%20Documents/ACP194.pdf

Declaration (IV,1), to Prohibit, for the Term of Five Years, the Launching of Projectiles and Explosives from Balloons, and Other Methods of Similar Nature. 29 July 1899, The Hague (entered into force 1909).

Department of Communication and the Arts. "Australian Government Held Spectrum Report." Last modified April 2019. https://www.communications.gov.au/file/48141/download?token=z_B0fkEy

Department of Defence. "Communication and Information Systems." Last modified 26 June 2012. https://www.defence.gov.au/adfwc/Documents/DoctrineLibrary/ADDP/ADDP_6-0_CIS.pdf

Eritrea–Ethiopia Claims Commission, Partial Award, Western Front, Aerial Bombardment and Related Claims, Eritrea's Claims 1, 3, 5, 9–13, 14, 21, 25 and 26 (2005) (P.C.A, 19 December 2005).

GATS: General Agreement on Trade in Services, 15 April, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994).

International Telecommunication Union. "Constitution of the International Telecommunication Union." In *Collection of the Basic Texts Adopted by the Plenipotentiary Conference*, 3–54. International Telecommunications Union, 2019.

International Telecommunication Union. "Convention of the International Telecommunication Union." In *Collection of the Basic Texts Adopted by the Plenipotentiary Conference*, 69–150. International Telecommunications Union, 2019.

International Telecommunication Union. "Radio Regulations." Volume 1, edition of 2020.

International Telecommunication Union. "Resolution 173 (Guadalajara, 2010): Piracy and Attacks Against Fixed and Cellular Telephone Networks," 692–693. In *Collection of the Basic Texts Adopted by the Plenipotentiary Conference*, 3–54. International Telecommunication Union, 2019.

International Telecommunication Union. "The 1865 International Telegraph Conference." Accessed 21 January 2020. https://www.itu.int/en/history/Pages/ITUBorn1865.aspx

International Telecommunication Union, "ITU-R: Managing the radio-frequency spectrum for the world.", Accessed 13 April 2021. https://www.itu.int/en.mediacentre/backgrounds/Pages/itu-r-managing-the-radion-frequency-spectrum-for-the-world.aspx.

International Telecommunication Union. *Economic Aspects of Spectrum Management*. June 2018. https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-SM.2012-6-2018-PDF-E.pdf

International Telecommunication Union. "Constitution and Convention." Accessed 21 January 2021. https://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx.

ITU Radiocommunication Assembly. "Recommendation 182–4: Automatic Monitoring of Occupancy of the Radio-Frequency Spectrum." Last modified 8 March 1992. https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.182-4-199203-S!!PDF-E.pdf

ITU Radiocommunication Assembly. "Recommendation ITU-R SM 1537: Automation and Integration of Spectrum Monitoring Systems with Automated Spectrum Management." Last modified 2001. https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.1537-0-200107-S!!PDF-E.pdf

ITU Radiocommunication Assembly. "Recommendation ITU-R SM.182–5: Automatic Monitoring of Occupancy of the Radio-Frequency Spectrum." Last modified 10 February 2007. https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.185-200702-W!!PDF-E.pdf

Jeanty, Lilian. "The Radio Regulations Board and WRC-19" ITU News. Last modified 24 October 2019. https://news.itu.int/the-radio-regulations-board-and-wrc19/

Law and the Future of War Research Group. "Submission to the ADF Concept for RAS 2040." University of Queensland. Last modified 31 July 2020. https://www.defence.gov.au/VCDF/Forceexploration/_Master/docs/Submission-to-the-RAS-2040-13August2020.pdf

LS Telecom. "Smart Solutions in Spectrum Management." Accessed 5 November 2020. https://www.lstelcom.com/en/solutions-in/spectrum-management

Ministry of Defence. "UK Defence Spectrum Management." Last modified 5 September 2008. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/35937/dsm_consultation_report.pdf

NATO Standardization Office. "Spectrum Management Allied Data Exchange Format – Extensible Markup Language." ASP-02, version 1, edition A. 2019. http://www.smadef.net/ASP02.pdf

Progira. "Spectrum Management." Accessed 5 November 2020. https://www.progira.com/spectrum-management/

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 1125 U.N.T.S. 3 (1977).
Radiocommunication Sector of ITU. "Design Guidelines for Developing Automated Spectrum Management Systems." Recommendation ITU-R SM. 1370–2. August 2013. https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.1370-2-201308-I!!PDF-E.pdf
Radiocommunication Sector of ITU. "Handbook on Computer-Aided Techniques for Spectrum Management (CAT)." Edition of 2015. https://www.itu.int/dms_pub/itu-r/opb/hdb/R-HDB-01-2015-PDF-E.pdf
Royal Australian Air Force. "EA-18G Growler." https://www.airforce.gov.au/technology/aircraft/strike/ea-18g-growler.
TCI. "Spectrum Management." Accessed 5 November 2020. https://www.tcibr.com/spectrum-management/
Trusted Autonomous Systems Defence CRC. "Projects." Accessed 5 November 2020. https://tasdcrc.com.au/projects-activities/
TSA Spectrum de Argentina SA v Argentine Republic, ICSID Case No. ARB/05/5 (29 December, 2008). https://www.italaw.com/sites/default/files/case-documents/ita0874.pdf
US Department of Defense. "Electromagnetic Spectrum Superiority Strategy". Released 19 October 2020. https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF
US Cybersecurity and Infrastructure Security Agency. "Radio Frequency Interference Best Practices Guidebook." February 2020. https://www.cisa.gov/sites/default/files/publications/safecom-ncswic_rf_interference_best_practices_guidebook_2.7.20_-_final_508c.pdf
Wrap International. "Spectrum Management and Monitoring System." Accessed 5 November 2020. https://wrap.se/spectrum-management-monitoring/introduction-spectrum-management/

Secondary Sources

"Chapter One: Defence and Military Analysis." *The Military Balance* 120, no 1 (2020): 9–20.
Alvarez, José E. *International Organizations as Law-Makers*. Oxford: Oxford University Press, 2005.
Britannica. "Electromagnetic Spectrum." Accessed 4 November 2020. https://www.britannica.com/science/electromagnetic-spectrum
Britannica. "Military Communication." Accessed 4 November 2020. https://www.britannica.com/technology/military-communication
Chan, Serena. "Shared Spectrum Access for the DoD." *IEEE Communications Magazine* 45, no 6 (2007): 58–66. https://doi.org/10.1109/MCOM.2007.374433
Congressional Research Services. "Defense Primer: Military Use of the Electromagnetic Spectrum." Last modified 8 October 2020. https://fas.org/sgp/crs/natsec/IF11155.pdf
Couture, Marc. "New Weapons in Battle to Dominate Spectrum." Signal. Last modified 1 August 2017. https://www.afcea.org/content/new-weapons-battle-dominate-spectrum
Crootof, Rebecca and B.J. Ard. "Structuring Techlaw." *Harvard Journal of Law & Technology* 34. Published ahead of print, 14 September 2020. https://dx.doi.org/10.2139/ssrn.3664124
Deloitte. "Mobile Nation: The Economics and Social Impacts of Mobile Technology." Last modified February 2013. https://amta.org.au/files/Mobile.nation.The.economic.and.social.impact.of.mobile.technology.pdf
Dinstein, Yoram. *The Conduct of Hostilities under the Law of International Armed Conflict*. 3rd ed. Cambridge: Cambridge University Press, 2016.
Gisel, Laurent, Tilman Rodenhauser and Knut Dormann. "Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflict." *International Review of the Red Cross*. Published ahead of print, September 2020. https://international-review.icrc.org/sites/default/files/reviews-pdf/2020-10/Twenty-years-on-IHL-and-cyber-operations-final-version.pdf
Hair, Jonathan. "Bureau of Meteorology Impacted by Internet Service Providers' Move to Wireless Frequency." *The World Today*, 16 May 2018. https://www.abc.net.au/news/2018-05-16/bom--radio-frequency-government-sell-off/9767000.
Harvard Program on Humanitarian Policy and Conflict. *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare*. Cambridge: Cambridge University Press, 2013.
Henckaerts, Jean-Marie and Louise Doswald-Beck. *Customary International Humanitarian Law*. Cambridge: Cambridge University Press, 2005.
International Telecommunications Union. "Landmark Decisions from Guadalajara". Last modified November 2010. http://www.itu.int/net/itunews/issues/2010/09/47.aspx
Jakhu, Ram S. "Regulatory Process for Communications Satellite Frequency Allocations." In *Handbook of Satellite Applications*, edited by Joseph N. Pelton, Scott Madry and Sergio Camacho-Lara, 359–381. Cham: Springer International Publishing, 2017.

Jensen, Eric Talbot. "Cyber Warfare and Precautions against the Effects of Attack." *Texas Law Review* 88, no 7 (2010): 1533–1570.

Jensen, Eric Talbot. "War in Cities: Attackers have Rules to Follow. What About Defenders?" International Committee of the Red Cross. Last modified 16 March 2017. https://blogs.icrc.org/law-and-policy/2017/03/16/war-cities-attackers-rules-follow-defenders/

Koziol, Michael. "DAPRA's Grand Challenge is Over—What's Next for AI-Enabled Spectrum Sharing Technology?" IEEE Spectrum. Last modified 25 October 2019. https://spectrum.ieee.org/tech-talk/telecom/wireless/with-darpas-spectrum-collaboration-challenge-completed-whats-the-next-step-for-spectrum-sharing-technologies

Levin, Harvey Joshua. *The Invisible Resource: Use and Regulation of the Radio Spectrum*. Baltimore: John Hopkins Press, 1971.

Liivoja, Rain, Eve Massingham, Tim McFarland and Simon McKenzie. "Are Autonomous Weapons Systems Prohibited?" Trusted Autonomous Systems Game Changer. Last modified 9 September 2020. https://tasdcrc.com.au/are-autonomous-weapons-systems-prohibited/

Liivoja, Rain and Tim McCormack. "Law in the Virtual Battlespace: The Tallin Manual and the *Jus in Bello*." In *Yearbook of International Humanitarian Law Volume 15*, edited by Terry D. Gill, Robin Geiss, Robert Heinsch, Tim McCormack, Christophe Paulussen and Jessica Dorsey, 45–58. The Hague: Asser Press, 2014.

Massingham, Eve. "Radio Silence: Autonomous Military Aircraft and the Importance of Communication for Their Use in Peace Time and in Times of Armed Conflict Under International Law." *Asia-Pacific Journal of International Humanitarian Law* 1 (2020): 184–208.

Mayhan Joseph T. and Leon J Ricardi. "Physical Limitations on Interference Reduction by Antenna Pattern Shaping." *IEEE Transactions on Antennas and Propagation* 23, no 5 (1975) 639–646. https://doi.org/10.1109/TAP.1975.1141135

McCormack, Tim. "International Humanitarian Law and the Targeting of Data." *International Law Studies* 94 (2018): 222–240.

McDougal, Myres S., Harold D. Lasswell and Ivan A. Vlasic. *Law and Public Order in Space*. London: Yale University Press, 1963.

Mountin, Sarah. "The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals." *International Law Studies* 90 (2014): 101–197.

Noll, Alfons A.E. "The ITU in the 21st Century." *Singapore Journal of International and Comparative Law* 5 (2001): 63–70.

Ofcom. "Spectrum Framework Review: The Public Sector." Last modified 12 July 2007. https://www.ofcom.org.uk/__data/assets/pdf_file/0018/29106/sfrps.pdf

Pandit, Shweta and G. Singh. "An Overview of Spectrum Sharing Techniques in Cognitive Radio Communication System." *Wireless Networks* 23 (2017): 497–518. https://doi.org/10.1007/s11276-015-1171-1

Panhans, David et al. "The Coming Battle for Spectrum." Boston Consulting Group. Last modified 11 February 2020. https://www.bcg.com/publications/2020/coming-battle-for-spectrum.

Rizer, Kenneth R. "Bombing Dual Use Targets: Legal, Ethical and Doctrinal Perspectives." *Airpower Journal* (2001). https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/Rizer.pdf

Roberts, Lawrence. "A Lost Connection: Geostationary Satellite Networks and the International Telecommunications Union." *Berkley Technology Law Journal* 15, no 3 (2000) 1095–1144. http://dx.doi.org/10.15779/Z38DQ1J

Sands, Philippe and Pierre Klein, eds. *Bowett's Law of International Institutions*. London: Sweet & Maxwell, 2001.

Sandoz, Yves, Christophe Swinarski and Bruno Zimmermann, eds., *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva: Martinus Nijhoff, 1987.

Sassòli, Marco and Anne Quintin. "Active and Passive Precautions in Air and Missile Warfare Section I: Air and Missile Warfare: Part A: Targeting and Protection." *Israel Yearbook on Human Rights* 44 (2014): 69–124.

Savage, James. *The Politics of the International Telecommunications Regulation*. Colorado: Westview Press, 1989.

Schmitt, Michael. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

Schmitt, Michael. "Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations." *International Review of the Red Cross* 1010 (2019): 333–355.

Selvadurai, Niloufer. "Enhancing the Effectiveness of Telecommunications Access Regulation: Moving From a 'Negotiate-Arbitrate' to an 'up-Front Decision' Model." *Australian Business Law Review* 39, no 5 (2011): 297–308.

Tilghmann, Paul. "AI Will Rule the Airwaves: A DARPA Grand Challenge Seeks Autonomous Radios to Manage the Wireless Spectrum." *IEEE Spectrum* (June 2019): 29–34.

Wang, Ximing, et al. "Machine Learning Empowered Spectrum Sharing in Intelligent Unmanned Swarm Communication Systems: Challenges, Requirements and Solutions." *IEEE Access* 8 (May 2020): 89839–89849. https://doi.org/10.1109/ACCESS.2020.2994198

Primary Legal Material

Defence (Special Undertakings) Act 1952 (Cth) (Aust.).
Defence Act 1990 (New Zealand).
Deutsche Telekom AG v Republic of India (Interim Award), PCA Case No. 2014–20 (13 December 2017).
Prosecutor v Kupreskić, Judgment, IT-95-16-T (I.C.T.Y., 14 January 2000).
Radiocommunications Act 1983 (Cth) (Aust.).
Radiocommunications Act 1992 (Cth) (Aust.).
Radiocommunications Act R.S.C. 1985, c. R-2 (Can.).
Responsibility of States for Internationally Wrongful Acts, GA Res 56/83, UNGAOR, 56th sess, 85th plen mtg, Supp No 49, UN Doc A/RES/56/83 (28 January 2002, adopted 12 December 2001) annex.
Telecommunications (Interception and Access) Act 1979 (Cth) (Aust.).
Title 47 Telecommunications (1943) U.S.C.
Wireless Telegraphy Act 2006 c. 36 (Eng.).