STRATEGIC INSIGHTS

ASPI

Somebody might hear us

Emerging communications security technologies

161

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

TWENTY YEARS OF ASPI STRATEGY 2001 - 2021

Andrew Davies

Introduction

Communications have always played a key role in military command and control, but the advent of smart weapons, remotely operated systems and network-centric warfare models has led to a huge increase in demand for reliable and secure communications channels. Today, there can be intercontinental distances between a commander and deployed battlefield sensors and shooters. Network operators need to guard against possible adversary actions such as intercepting or jamming signals, or perhaps inserting bogus information into their communications network and information systems. In tactical and operational settings, sometimes even the fact of a communication—even if it is unintelligible to a foe—needs to be kept hidden to avoid flagging presence or providing clues about operational activity. One way to do that is to keep communications entirely in secure physical channels that the adversary can't access, such as protected fibre-optic cables, but a dispersed military force doesn't have that luxury. Therefore, there continues to be a requirement for radiated secure communication channels.

Australian army soldier signaller Nathaniel Whittaker from 145th Signals Squadron, which is part of 17th Combat Signal Regiment, provides communication support during Exercise Hamel in Cultana training area, South Australia, 3 July 2016. Defence image library, online.

May 2021

In an ideal world, communications would be cheap, reliable, easy to use, secure and robust against disruption and have unlimited bandwidth. In practice, as with virtually every military capability sought, trade-offs between the desirable characteristics are inevitable, and realistic acquisition processes need to balance that reality. However, for communications technology the cost versus capability trade-off is increasingly favourable—and that makes it very much unlike most other military capabilities. While government R&D has played a role in developing past military information and communications technologies (ICTs), especially in the Cold War period, today innovation is increasingly driven by the commercial sector and leveraged by military purchasers. The huge global market for ICT products attracts R&D investments that far exceed government R&D budgets, and the net result has been decades of unbroken exponential improvement in both processing speed and accessibility to bandwidth. Those advances have enabled new operational concepts in the modern dispersed and disaggregated battlespace. Militaries are increasingly networking a wide range of inhabited and remotely operated mobile nodes that can operate together to widen the sensor network to improve their C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) capabilities.

Despite predictions at various times that the exponential growth of communication capability is about to come to an end, innovative approaches to the use of existing technology (such as various approaches to multiplexing) have increased the effective capacity of existing devices, and new hardware has emerged as previous technological paths reached their natural limits. There's no sign of an imminent slowdown; future generations of communication systems and the computing systems with which they will increasingly be integrated will enable new operational approaches that are yet to be invented.

Improvements in communications capabilities can come from increases in bandwidth and data rates, additional security, or better resilience between network elements. The focus here is on the security of communications in non-fixed networks, and this paper sets out a framework for a 'defence in depth' approach to securing communications. It describes some promising emerging communication technologies and techniques (as well as some innovative new approaches to using established technologies) that will enable such an approach. It isn't intended to be a comprehensive technology survey, but the examples provided illustrate the sorts of approaches that might appear in future military communication systems.

The desired characteristics of secure communications

Within defence circles, there's often a tendency to regard 'information security' as a synonym for encryption, and to think that all that's required is having access to a suitably certified 'black box' through which communications will pass. But history has shown that relying solely on encryption for security is often inadequate: supposedly secure cipher systems have sometimes yielded their secrets to cryptanalysis, aided by some combination of systemic weaknesses, operator error or betrayal by trusted insiders or simply because the adversary was more capable than they were given credit for. Rather than relying solely on encryption, a secure communications network should rely on defence in depth, with a view to making life as hard as possible for an adversary at multiple steps. With that perspective, in this paper we break down communications security into three broad approaches:[1]

- reducing the probability of a signal being detected (LPD—low probability of detection)
- reducing the probability of a signal being accurately or completely collected, given that it's detected (LPI—low probability of intercept)
- reducing the probability of a signal being exploited, including by encrypting the content, given that it is detected and collected.

Though cybersecurity is beyond the scope of this paper, we note that it should be considered as an important part of a holistic approach to information security. The convergence of communication and computer technology means that data now needs to be secured when at rest in computers at either end of the channel, as well as when in transit.

While security is a necessary feature of a military communications network, other characteristics are required for operational effectiveness, including the provision of adequate bandwidth—which is often in short supply when multiple force elements are operating concurrently. As we'll see, there are technologies on the horizon that promise to deliver both greater levels of security and higher data rates. And that's just as well, as a combination of the technical advances and the increased sophistication of regional players means that the potential threat to the communications security of Australia and our allies is increasing.

The threat

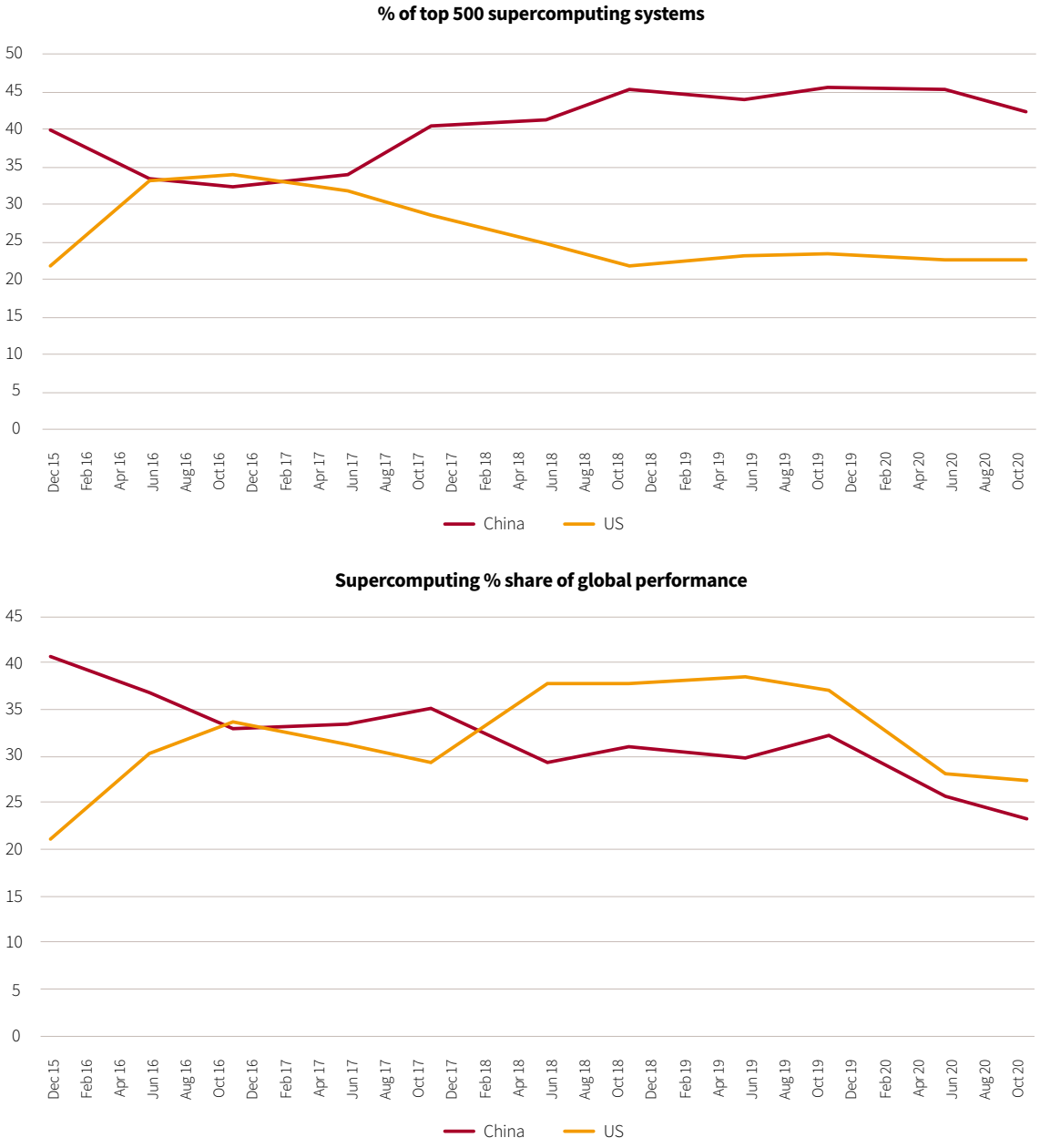
Military modernisation in the Asian region over the past few decades has meant that regional forces have increased their capabilities across the board. As well as acquiring advanced platforms, which often come with sophisticated integrated C4ISR and electronic warfare capabilities, regional militaries have also become increasingly able to both secure their own communications and exploit those of other nations. Australia has been fortunate in being part of the US alliance network, which has allowed it to be a highly successful collector and user of signals intelligence, as well as providing access to advanced communications security methods and systems. But there are indicators that the information superiority that Australia and our allies have been able to assume when planning operational activities is coming under significant challenge. In particular, the rise of the People's Republic of China (PRC) as a major power raises the prospect of having to operate against a peer adversary in the information domain.

As part of its aspiration to first blunt and then match US military and national capabilities, China's People's Liberation Army (PLA) has long stated an aspiration to be able to dominate the electromagnetic spectrum and to be able to operate in an environment of what successive Chinese defence white papers have called 'informationalisation'. The PLA's force modernisation efforts include building a C4ISR infrastructure that allows it to move data between mobile platforms, collection points and processing centres. While the PRC doesn't have the global capabilities of the Five Eyes nations and their allies, it's been building a signals intelligence architecture that provides a robust collection capability in and around its own territories, including ground-based collection sites positioned to collect satellite communications to Russia, India, Taiwan and other neighbouring states.[2] China also has national space-based collection capabilities. There's an elaborate organisational structure behind the signals intelligence effort, and the overall Chinese technical intelligence workforce has been estimated to be well over 100,000.

Consistent with its broad strategic approach of consolidating its immediate territory and then working to extend its power outwards, China is now forward-deploying a range of signals collection sites, as well as extending its fleet of ships and aircraft capable of collecting signals ranging from line-of-sight tactical communications to satellite downlinks. As a result of its development activities in the South China Sea this century, the PLA now has both fixed and mobile signals collection assets based there, allowing it to collect intelligence all the way from Japanese airspace in the north to Indonesia in the south.[3] The fixed sites on islands and shoals in the South China Sea include radio frequency (RF) direction-finding installations and dishes for collecting satellite communications. The mobile collection assets include electronic warfare aircraft that also have jamming capabilities. The PLA's doctrine for 'working in a complex electromagnetic environment' involves both signals intelligence and electronic attack, both of which work alongside active (attack) and passive (collection) computer network activities.

Four years ago, China held the top two positions (ranked by the number of operations per second) on the Top 500 supercomputer list and had equalled the US for the number of entries on the list (171 each). The most recent figures, released in November 2020,[4] show that the top spots are now held by Japanese and American systems, but in terms of numbers of high-performance designs the PRC now dominates the list, with 42.4% of the entries. As shown in Figure 1, the US is in second place with only a little over half that number (22.4%). The situation is less stark when the figures are weighted by aggregate system performance (that is, the total number of operations a nation's supercomputer inventory can process each second), in which the US (27.5%) and China (23.2%) are near peers (Japan has recently achieved a similar performance share).

Figure 1: Supercomputing capability of the US and China, ranked by the number of systems in the top 500 (top) and by share of aggregate global performance (bottom)



Source: Top500.org

Overall, the PRC has, and continues to further develop, the capability to collect a broad range of signals intelligence and move the collected data around over secure networks. It has a significant capacity to process and exploit signals, including being able to attack protected information with an amount of supercomputing power on a par with that of the US. When developing communications security policy, Australia and our allies and partners should make the prudent planning assumption that Chinese signals intelligence is capable of doing anything that we can do.

Low-probability-of-detection communications

One way of keeping communications from an adversary is to never have them pass over channels that are susceptible to detection or interception. That isn't always possible for mobile force elements but, when it is, communications security can be very effective. In the lead-up to its Ardennes offensive in December 1944, the German army greatly reduced its radio transmissions, relying instead on couriers and landlines run within the territory it occupied (which was contiguous with Germany, so that command and control traffic could mostly be kept off the airwaves). Allied intelligence—lulled into complacency by hitherto consistently having forewarning of German movements from intercepted radio traffic—missed the build-up of substantial German forces and was taken by surprise. The ability to go 'off air' when circumstances allow is still worth having, especially today, when fibre-optic cables can carry data at much higher rates than copper cables.

Of course, mobile forces often won't have the luxury of being able to move all traffic onto cables, especially in fast-moving situations, but there are still ways to greatly reduce the footprint of communication signals and, in some instances, to render them effectively immune to detection. Previous approaches to making signals less obvious to a would-be eavesdropper included frequency-hopping and spread-spectrum radios. Those techniques indeed reduce the RF footprint of signals, but today are susceptible to detection, interception and exploitation through the use of wideband receivers and computer spectral analysis tools.

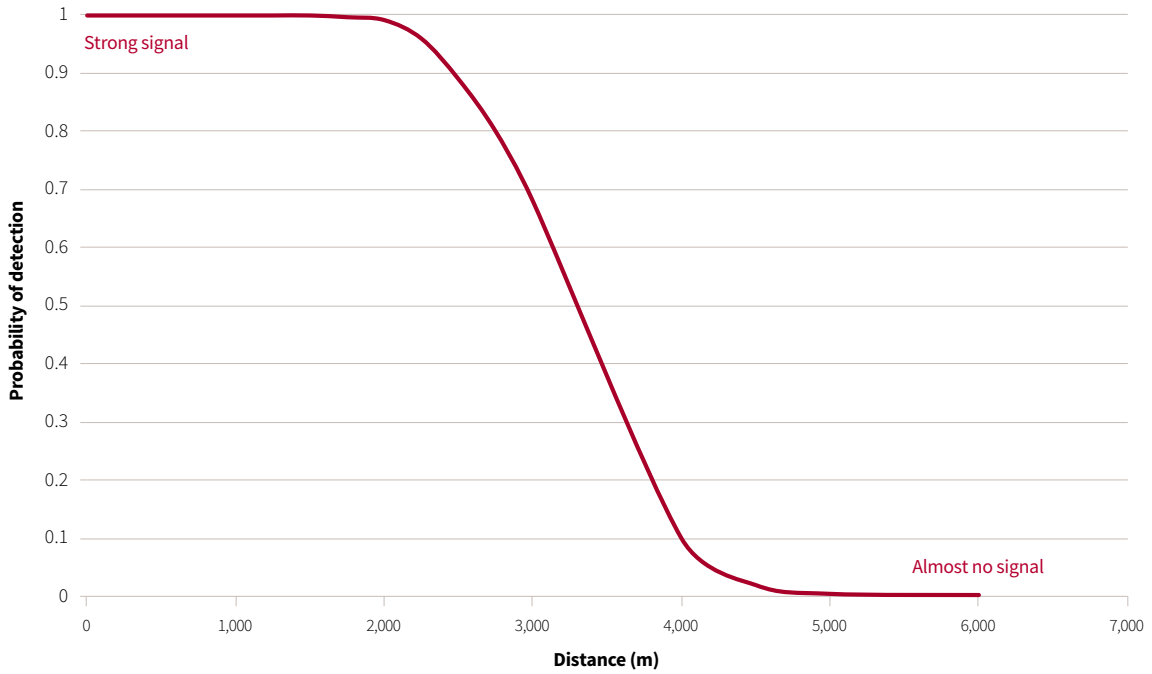
Emerging technologies provide a number of new ways of achieving the same goal, but with greater security. The first is to employ highly directional 'line of sight' signals that can be aimed towards the intended recipient, thus curtailing the ability of an adversary to even detect the transmission. That might be done, for example, via tightly focused laser signals of various wavelengths, which can—when geography permits—be precisely aimed at the intended recipient's antenna. Alternatively, a space-based relay, in which two or more force elements are linked by laser communication channels with a constellation of satellites, which are themselves connected by secure links (see the next section for examples of active work in that area), provides a communications path that's hard to intercept. The net result would be the ability to exchange data with much less risk of detection than for RF signals. A satellite system with a global footprint for its uplinks and downlinks has effectively no limit on the distances between the communicating parties.

A second approach, more suited to force elements in close proximity, is to move radio transmissions to wavelengths that don't propagate over long distances because of atmospheric absorption, but which still provide robust communications capability at short ranges. For example, the US Army has an active research program into deep ultraviolet communications (UVC).[5] The advantages of UVC over radio frequencies such as UHF and VHF are that:

- the higher frequency allows for more rapid transmission of data
- over short ranges, relatively low-powered signals may still be easily received
- there's a rapid fall-off of signal strength at a critical distance.

Figure 2 shows some modelled numbers for a low-power UVC system: the probability of detection is high at ranges of up to a couple of kilometres (a desirable trait for communicating with friendly forces) but falls off rapidly after that. A patient adversary can integrate weak signals over extended periods (minutes to hours) to improve the signal-to-noise ratio if there are sufficient transmissions, but even then only modest gains in detection range are possible.

Figure 2: A simplified representation of the fall-off of the probability of detection of a UV signal as a function of distance; reception is almost guaranteed within 2 kilometres of the emitter, but real-time detection is unlikely at more than 4 kilometres



Source: Adapted from Figure 6 in Michael J Weisman, Fikadu T Dagefu, Terrence J Moore, C Hakan Arslan, Robert J Drost, 'Analysis of the low-probability-of-detection characteristics of ultraviolet communications', *Optics Express*, 2020, 28(16):23640–23651, online.

A current way of securing short-range communications is by using directional transmitters and antennas. That's a valid approach if point-to-point communication between isolated entities is the goal, but UVC would also allow for broadcasts to many parties within a radius of several kilometres (for example, to and from all elements of a deployed land force element). Clearly, an adversary with a collection capability that's almost co-located with the communicating parties would be able to detect and possibly intercept the communications, but the area needing to be secured would be limited.

The same idea lies behind a 2019 request for tender (RFT) issued by the US Navy for a line-of-sight LPD/LPI millimetre wave communication system for its F/A-18 Hornets and Super Hornets (which is clearly also of interest to the ADF).[6] By using millimetre waves (in the part of the spectrum where microwaves and infra-red radiation overlap), high data rates are possible but, as with the UV example above, atmospheric absorption prevents propagation beyond a few kilometres. The intended application seems to be data exchange between nearby aircraft, as the RFT gives as a performance goal 'a minimum data throughput of 1 Gb/s at 1 nautical mile under all weather conditions'.

Another approach worth mentioning here is hiding signals within a noisy background—again an area in which the US Department of Defense has an active interest. In 2019, the Small Business Innovation Research (SBIR) agency issued a solicitation for building and demonstrating a 'low probability of detection, low probability of intercept "noisy" RF communication system' for the US Army.[7] The work draws on earlier successful demonstrations of the production of radar signals composed of pseudo-randomly generated random RF signals that are practically undetectable against a truly random noise background. The solicitation says that the goal of the project

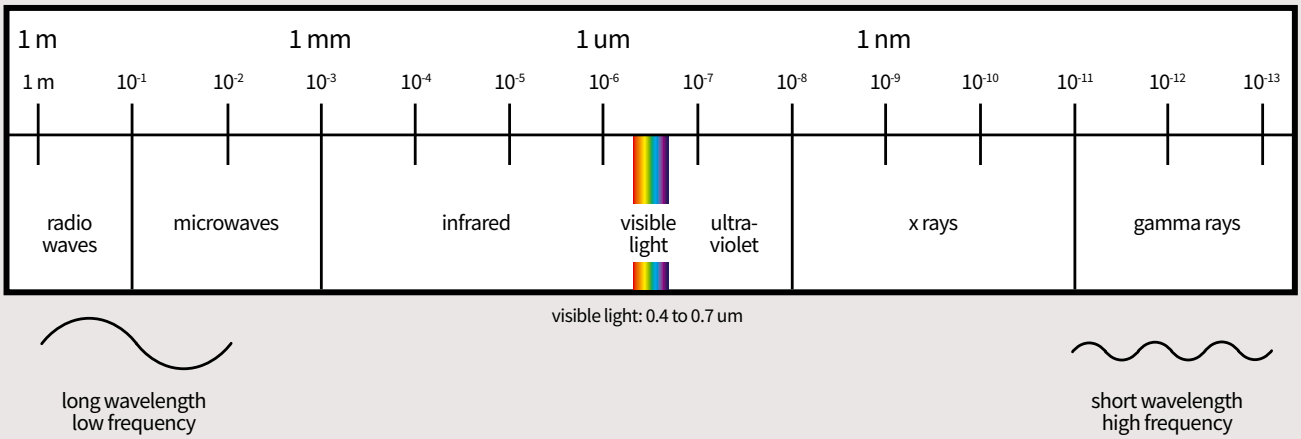
> … is to demonstrate the application of a noisy RF system which can provide voice and data communications across several systems. While the primary goal is to build and test a clandestine communication system, the program will also research the optimal frequencies, bandwidth constraints and other relevant factors effecting a clandestine RF based mobile communication network.

(The solicitation closed in October 2019, but no contract award has yet appeared in the SBIR database.)

Frequencies, transmission distances and data rates

One way to increase transmission data rates is to move to higher frequencies in the electromagnetic spectrum. Broadcast radio and television transmissions are in the range of 1 MHz to 1 GHz, and microwave communications and radar systems operate in the 1–100 GHz range (Figure 3). Moving to higher frequencies (shorter wavelengths) allows for more data to be encoded in modulation per unit time. And, because of the reduced size of the antennae required, it's easier to tightly collimate directional beams at higher frequencies, thus saving on power and reducing interception possibilities.

Figure 3: The electromagnetic spectrum



But there are also offsetting disadvantages for broadcast systems. In particular, higher frequency radiation tends to interact more strongly with atmospheric matter, reducing the distances over which signals can be reliably sent. For example, although they're capable of sustaining higher data rates than RF signals, the microwave communications used in mobile telephony networks are confined to frequencies at which microwaves are not strongly absorbed by water vapour in the atmosphere. For still higher frequencies, some atmospheric 'frequency windows' exist, allowing for long-distance propagation paths, but those tend to become narrower, and moving to higher frequencies generally further exacerbates that problem.

The infra-red part of the spectrum (frequencies around 1–100 THz) is at a higher frequency than microwaves. Although there's almost complete absorption of infra-red radiation by the atmosphere at some frequencies, there are some windows that allow long-distance transmissions, including to and from orbit (which is also important in the study of greenhouse gases.) Beyond the visible spectrum, most UV radiation is strongly absorbed (see the main text for how that can be exploited for secure short-distance communications), and even higher frequency X-rays have very short propagation lengths due to the ionisation of atmospheric gases.

Space-based links as secure intermediaries

Space-based communications potentially provide a secure communication channel for terrestrial entities, provided that the links can be rendered uninterceptable. Until now, communication of information and control signals between spacecraft and the Earth has been via radio waves to and from ground stations. While the collimation of RF uplinks and downlinks is possible, interception is possible when collection systems are near enough to the uplink transmitter to collect energy from either the unavoidable side lobes of the main beam or when the collection system is able to be located within the same downlink footprint as the receiver. Replacing those RF links with laser signals of various wavelengths has the potential to simultaneously improve data rates and to secure the signals against interception.

As well, there are significant advantages to using laser communication links between spacecraft. RF links necessarily limit bandwidth, and transmission losses over large distances limit the efficiency with which spacecraft with tight power budgets can communicate large volumes of data. Replacing those links with laser communications would reduce the imposts on space, weight and power on spacecraft. The payoffs from that would include being able to carry larger sensor and processing payloads, a higher proportion of time on mission (due to less downtime to recharge batteries being required), or some combination of both. In the US, the Trump administration's Space Force and proposed NASA activities (including a presence on the moon and deep space missions) have spawned a number of research programs aimed at developing new space-based communications systems.

NASA has a decade-long project road map (the 'decade of light'[8]) that's aimed at developing infra-red and optical frequency laser communication systems, integrating them with RF systems and connecting multiple sites and spacecraft into a robust damage-resistant network. It has several technology demonstrators underway as part of that program. Its Laser Communications Relay Demonstration, due to launch in June this year, uses lasers to encode and transmit data at rates 10 to 100 times those of radio systems.[9] As an example of the possible efficiency benefits, NASA cites the example of transmitting a map of the surface of Mars back to Earth, which might take nine years with current radio systems but as little as nine weeks with laser communications. Laboratory prototype systems have proven the feasibility of laser communications, and NASA is to launch space-based prototypes later this year.

Both the Defense Advanced Research Projects Agency (DARPA) and the Pentagon's Space Development Agency (SDA) are thinking along similar technology lines, but with military and intelligence applications in mind. The SDA envisages a constellation of hundreds of satellites connected by infra-red and optical laser communication links.[10] The idea is for the constellation to pass sensor information between spacecraft until it reaches a satellite in contact with a ground station. Information from an orbiting sensor grid can therefore be brought to Earth in subsecond time frames, rather than requiring the sometimes tens of minutes for a particular low Earth orbiting satellite to come within the line of sight of a ground station. As well, the tight beams formed by lasers means that there's very little opportunity for an eavesdropper to intercept the communication. The communication efficiency also means that the 'traffic jams' that occur in the relatively more heavily used radio spectrum are much less likely to occur. The SDA is planning a test with a small number of 'cubesats' this year.

Moving to higher frequencies still, beams of X-rays could in principle carry very high data-rate signals. Ionisation of atmospheric gases would quickly attenuate the signals in terrestrial applications, but that isn't an issue in space, and NASA is now working on gigabits-per-second X-ray data links between spacecraft.[11] NASA's interest is primarily in applications for deep space missions (current methods can take many hours to transmit a single high-resolution photograph of a distant object such as an asteroid after a flypast), but the technology also has the potential to link future constellations of intelligence-gathering and communications satellites with very high data-rate channels. NASA has deployed a technology demonstrator on board the International Space Station.

If all else fails … encryption systems for the 21st century

As discussed above, one way to add security to communications is to be able to 'narrowcast' in a way that makes interception physically difficult, if not impossible. But that isn't always possible, and there will always be communications that have to travel via paths that make them vulnerable to eavesdropping. And even 'secure' paths can sometimes be unexpectedly compromised. A good example is the US Navy's physical tapping of a seabed cable run to a Soviet naval base on the Kamchatka Peninsula in the 1970s. Because the cable was entirely within Russian territorial waters and protected by underwater listening posts, it was considered secure and so carried unencrypted communications. Though not of high intelligence value in themselves, the collected signals provided cleartext 'cribs' of Soviet naval signals that could be compared with encrypted material collected elsewhere, greatly simplifying the cryptanalytic task.

And even some of the LPI/LPD technology systems mentioned in previous sections could be vulnerable to innovative new approaches. For example, the Pentagon has sponsored a research program into systems to detect laser transmissions from outside the beam by collecting single photons scattered off atmospheric particles, with a subsequent aim to then extract useful information about the beam direction, data rates and modulation type. The ultimate goal is eventually to be able to intercept laser transmissions.[12]

Prudent communications security practice should therefore be to assume that, despite efforts to make it as difficult as possible, an adversary will find a way to access communications. Highly sensitive information must be protected against the possibility of interception, and some material needs to be secure for years or even decades. There's a requirement for cryptographic techniques that render an intercepted message unreadable. As we saw in the section on the PRC's capabilities, very substantial computing power is already available to attack Australian and allied military communications, and that situation will worsen with time. And there are also technological threats on the horizon, the best known of which is the possible advent of practical quantum computing. 'Future proofing' of encryption is necessary.

Post-quantum encryption

Many popular media accounts of quantum computing suggest that the development of reliable large-scale quantum computers will spell the end of encryption and that quantum computers are just around the corner. The latter view may prove to be overoptimistic (or pessimistic, if you happen to rely on quantum-computing-proof security). While the technology has achieved some important milestones in recent years, there's no guarantee that quantum computers will move beyond laboratory proof-of-concept systems to become a practical everyday technology in the near future. (See a previous ASPI paper for a more detailed discussion.[13])

Nonetheless, if quantum computing does mature into a practical technology, some of the currently widely used encryption schemes are vulnerable to quantum computer cryptographic attacks because there are quantum algorithms that greatly reduce the time required to break them. For example, the RSA encryption scheme[14] for the secure sharing of encryption keys that underpins most web-based commerce is based on the practical difficulty of using classical (that is, non-quantum) computers to find the prime factors of very large numbers.[15] However, there's a very efficient quantum algorithm ('Shor's algorithm') for prime factorisation that would render RSA encryption vulnerable to attack, threatening the security of the large amount of economic activity that depends on being able to secure moving data. Other widely used encryption standards, such as the Digital Signature Algorithm (DSA) and Elliptic Curve DSA, also rely on mathematical steps that are classically difficult to reverse but that may be susceptible to quantum computing attacks.

One way to secure communications would be to move to secure quantum communication channels. But, while point-to-point quantum channels are feasible (and resistant even to quantum computer attacks), they have relatively high management overheads, and there are practical difficulties in establishing a quantum 'web' configuration. For applications such as networking military force elements, establishing secure links between intelligence agencies and setting up a secure wide-area network, a classical solution is likely to be preferred for some time to come. Happily, there are also non-quantum (classical) approaches to data security that are likely to remain secure even against quantum computer attacks. For example, the 256-bit Advanced Encryption Standard (AES-256) commonly used to secure sensitive information at rest has been shown to be resistant to quantum attacks.[16]

Protecting information at rest solves only part of the problem, as there still needs to be a secure mechanism for sharing encryption keys between the start and end points for data on the move. As a result, there's a substantial body of work going on to develop 'post-quantum' encryption schemes that would rely on mathematical operations for which there are no known quantum algorithms. IBM has already described a quantum-resistant system that would allow data to be moved securely across networks.[17] Such a system could potentially replace RSA and other quantum-vulnerable encryption schemes if the need arises.

Considerations for future Australian communications security capability

The ADF will need to continue to build joint interoperability between its constituent services and with national authorities, as well as being able to work as seamlessly as possible with allied and coalition forces. The interest being shown by the US in many of the technologies described in this paper suggests that the ADF may have to follow suit to maintain interoperability. However, there's a risk in adopting some of the high-tech solutions discussed here, in that the ADF will end up far ahead of many regional militaries with which it will have to work in peacekeeping and humanitarian and disaster relief missions. While we wouldn't want to share our most sensitive encryption capabilities with regional partners, in a cooperative or coalition setting it would be useful if we were at least able to provide them with access to communications channels that are protected to the appropriate level.

Encryption is an area in which a level of sovereignty must be retained. That doesn't necessarily translate into being able to indigenously produce encryption equipment, but it does mean that we need to be able to scrutinise and possibly adapt foreign-sourced equipment to ensure that Australia's 'Australian eyes only' communications are not accessible to other parties, including allies. There are also regional communications systems from which the ADF may need to be able to collect and exploit information that might not be a high priority for our allies, meaning that an indigenous capacity to develop those capabilities would be advantageous.

Defence has plans to make considerable investments in the ADF's communications security infrastructure over the next decade and beyond. The initial steps will be remediations of current shortcomings. That will be followed by a modernisation phase, in which some new technologies are likely to be introduced. But, beyond that, there's a vision for a transformational approach to communications and security. As we've seen in this paper, there are many emerging technologies and techniques that could provide higher data rates than current systems while concurrently improving security. Many are already at the technology demonstrator stage, and others are under development contracts. Space-based systems are likely to play an even more important role in future communication architectures. If we get it right, the future ADF will have a level of secure networking far beyond that of its predecessor.

Notes

1 A similar conceptual framework can be found in the ASD publication ACSI 53F, *Safeguarding COMSEC material*, which defines communications security as 'all measures applied to protect government telecommunications from unauthorised interception and exploitation and to ensure the authenticity of such telecommunications'. It lists five attributes, including cryptosecurity and transmission security (TRANSEC). The dot-points here focus on the TRANSEC (all three points) and cryptosecurity (final point) elements.

2 John Costello, Joe McReynolds, *China's Strategic Support Force: a force for a new era*, Institute for National Strategic Studies, 2018, online.

3 J Michael Dahm, *Electronic warfare and signals intelligence*, South China Sea military capability series, John Hopkins University, 2020, online.

4 The relevant statistics are compiled at *Top 500: the list*, online

5 For some indicative numbers from a theoretical model of UVC, see Michael J Weisman, Fikadu T Dagefu, Terrence J Moore, C Hakan Arslan, Robert J Drost, 'Analysis of the low-probability-of-detection characteristics of ultraviolet communications', *Optics Express*, 2020, 28(16):23640–23651, online.

6 The RFT information can be found in *Line-of-sight (LOS) low probability of detection/intercept (LPD/LPI) millimeter wave communication*, Navy SBIR 2019.2, topic N192-091, Navy Small Business Innovation Research / Small Business Technology Transfer, US Government, 31 May 2019, online.

7 *Low-cost low-probability-detection low-probability of intercept & noisy RF communication system*, Small Business Innovation Research / Small Business Technology Transfer, US Government, 23 August 2019, online.

8 Philip Liebrecht, Donald Cornwell, David Israel, Gregory Heckler, 'The decade of light: innovations in space communications and navigation technologies', *Journal of Space Operations & Communicator*, 2019, 16(1), online.

9 There's an overview of the system on NASA's *Decade of Light* website, online.

10 Sandra Erwin, 'DoD to test laser communications terminals in low Earth orbit', *Space News*, 8 June 2020, online.

11 Lori Keesey, *NASA set to demonstrate X-ray communications in space*, NASA, 20 February 2019, online.

12 Small Business Innovation Research Agency solicitation for 'Detection and intercept of FSO interplane communications using long-distance transmission (DIFICULT)', 2018, online.

13 Andrew Davies, Patrick Kennedy, *From little things: quantum technologies and their application to defence*, ASPI, Canberra, 2017, online.

14 RSA = Rivest–Shamir–Adleman.

15 Susmita Bhowmick, 'What is the role of RSA in ecommerce', *Appseconnect*, 2017 online.

16 X Bonnetain, M Naya-Plasencia, A Schrottenloher, 'Quantum security analysis of AES', *IACR Transactions on Symmetric Cryptology*, 2019(2):55–93, online.

17 Sophie Bushworth, 'New encryption system protects data from quantum computers', *Scientific American*, October 2019, online.

Acronyms and abbreviations

ADF	Australian Defence Force
C4ISR	command, control, communications, computers, intelligence, surveillance and reconnaissance
DARPA	Defense Advanced Research Projects Agency (US)
DSA	digital signature algorithm
ICT	information and communications technology
LPD	low probability of detection
LPI	low probability of intercept
PLA	People's Liberation Army
PRC	People's Republic of China
R&D	research and development
RF	radio frequency
RFT	request for tender
SBIR	Small Business Innovation Research (US)
SDA	Space Development Agency (US)
UHF	ultra-high frequency
UVC	ultraviolet communications
VHF	very high frequency

About the author

Dr Andrew Davies is a Senior Fellow at ASPI. He was the inaugural Director of ASPI's Defence & Strategy Program until March 2018.

About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our annual report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

Important disclaimer

About Strategic Insights

Strategic Insights are short studies intended to provide expert perspectives on topical policy issues. They reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI

Tel +61 2 6270 5100
Fax +61 2 6273 9566
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

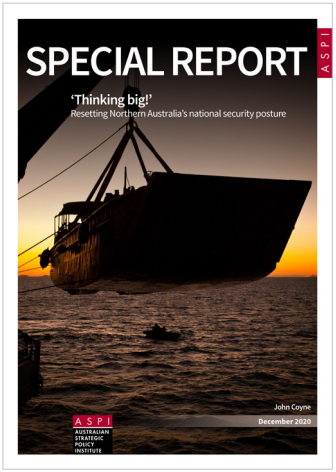
facebook.com/ASPI.org

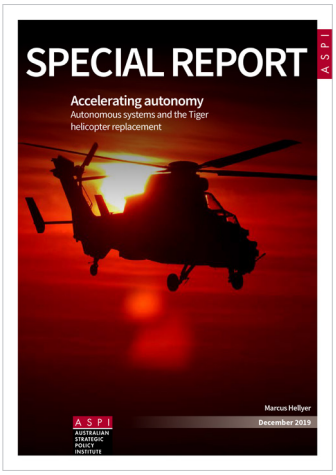
@ASPI_org

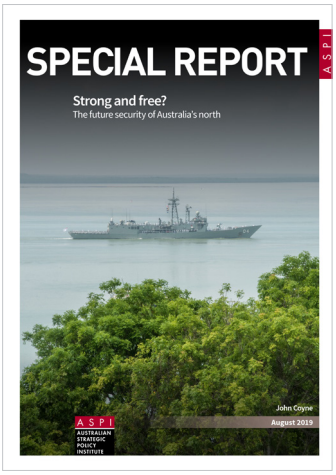
ISSN 1449-3993

This report was produced with funding support from the Department of Defence.

Some recent ASPI publications







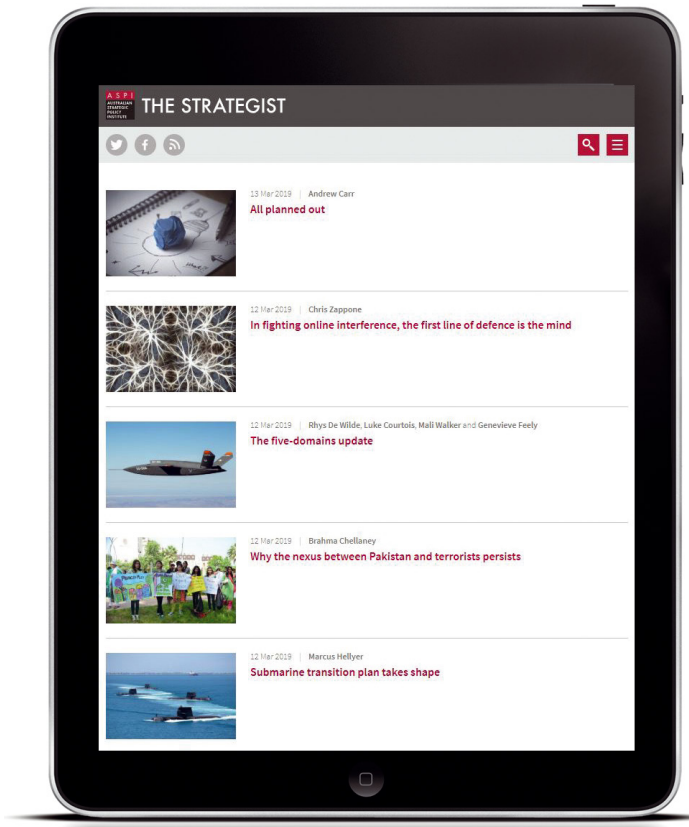
WHAT'S YOUR STRATEGY?

Stay informed via the field's leading think tank, the Australian Strategic Policy Institute.

The Strategist, ASPI's commentary and analysis website, delivers fresh ideas on Australia's defence and strategic policy choices as well as encouraging discussion and debate among interested stakeholders in the online strategy community. Visit and subscribe to an email digest at www.aspistrategist.org.au.

facebook.com/ASPI.org

@ASPI_org



ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Supported by

LOCKHEED MARTIN THALES NAVAL GROUP

To find out more about ASPI go to www.aspi.org.au or contact us on 02 6270 5100 and enquiries@aspi.org.au.

Somebody might hear us

Emerging communications security technologies