AUKUS – Cyber Security Aspects

Vijay Varadharajan
Global Innovation Chair Professor and Chief Cyber Strategist
Director: Advanced Cyber Security Research Engineering Centre (ACSRC)

We all know AUKUS is a trilateral security pact between Australia, the UK and the US, announced in Sept 2021. Under this pact, Australia will acquire nuclear powered submarines from the UK and the US.

But AUKUS is much more than just nuclear submarines. It is much broader than that, with a focus on the security of the Indo-Pacific region. Both our PMs before and after the recent election have referred to AUKUS as being a comprehensive agreement covering interoperability of defence assets between the partners.

The pact is intended to include cooperation on advanced technologies such as cyber, artificial intelligence, autonomous systems and quantum technologies. And the focus is more on the military and defence capabilities, separating it from the Five Eyes intelligence sharing alliance which also includes New Zealand and Canada.

There have been several statements in the public media about AUKUS including -- AUKUS will enable game changing technology transfer, potentially creating opportunities not only for Australian Defence but also for Australian businesses in general, for instance, in the context of regulatory frameworks both within and between AUKUS alliance partners.

I would like to explore cyber aspects that are relevant to AUKUS, and which could and, in my view, perhaps should form part of AUKUS

Strategic Context of the Indo-Pacific

It has become a highly competitive environment and a more contested one with tension, and assertive posture by one country in the region, namely China, in the recent times.

A major driver is the strategic competition between the US and China. We have been witnessing a more assertive behaviour from China in the recent times in advancing its strategic preferences and seeking to exert greater influence in the Indo-Pacific region.

This strategic competition between the United States and China is unlikely to abate, and in fact, with the pandemic and the war in Ukraine and with the recent tension with Taiwan, this competition has sharpened even more.

If one looks at the general trend in the region, it is fair to say that there has been an acceleration of military modernisation in the region, which has been enabled by a period of economic growth. Though the pandemic has probably slowed down this military modernisation, it is likely this will be continued to be prioritised.

Such regional military modernisation includes things like the advancement in maritime surveillance, which clearly has implications for Australian operations in the region. New weapons being introduced into the region with increased range, speed, precision and lethality, potentially placing Australian military forces at greater risk over longer distances.

This brings me to another major factor namely disruptive technologies, which is influencing the strategic context of the region. These disruptive technologies are being translated into sophisticated weapons systems – such as autonomous systems – reducing decision times and improving weapon lethality. This also gives opportunities for non-state actors such as potential terrorists to adapt new technologies for their purposes.

All these have implications for security and peace in the region. Growing regional military capabilities, and the speed at which they can be deployed, mean reduced warning times. Reduced warning times mean defence plans can no longer assume that they will have time to

gradually adjust military capability and preparedness in response to the emerging challenges.

Furthermore, such strategic circumstances with greater competition between major powers in the region together with military modernisation and potential economic coercion can increase the potential for miscalculation and their adverse consequences.

All these are putting an increasing strain on the rule-based order which has been the cornerstone of foreign policies for many years. This is being further exacerbated with developments in domains such as space and cyber. In these domains, rules of engagement are not always clear, and the thresholds for triggering a military response are often confusing, and they lack the more clearly defined boundaries of national borders. Let us now look at more closely the implications for cyber security.

Implications for Cyber Security

When it comes to cyber, the strategic context provides the opportunity for the increasing willingness by some countries and non-state actors to use the cyber capabilities maliciously. At a broad level, cyberattacks directly compromise military capability and operations. They drive disinformation with a destabilising interference to the society and the economy, and political systems. They are often conducted in ways designed to facilitate deniability and complicate attribution. And cyberspace transcends borders, making it easier for attackers and rogue states to carry out these cyberattacks.

Technology Scenery and Cyber Security

It is clear technology is pervasive, and so is cyber security. Anywhere there is technology there can be aspects of security, privacy, and trust.

If we look at the technology scenery, we have different types of networks (such as fixed, wireless, and mobile networks), large scale distributed systems and cloud services (these are fixed). Then there is mobile software (such as mobile apps). Then there are small devices such as sensors and Internet of Things, to large scale data centres, distributed databases, and infrastructures.

So, we have various technologies and platforms in a melting pot, in fact, a spaghetti of heterogeneous technologies, creating a pervasive distributed mobile environment.

Then there are users. Just like technology, it is not a monolith and there are different types of users, from individuals, small to medium enterprises (SMEs), to large corporations and government agencies. They all have different types of user requirements.

Various aspects of security, privacy and trust arise with each of these technologies and types of users.

Characteristics of Cyber Security

At a high level, cyber security is the application of technologies, processes and controls to protect systems, networks, devices, data and users from threats and attacks.

Security is relative to threats being perceived and the threats are dynamic. As threats constantly evolve, there is a need for secure systems to be continuously updated to counteract new and emerging threats.

We can think of cyber threats as possible attacks on a system or some digital asset. Threats exploit vulnerabilities and vulnerabilities materialize as risks.

There will be some residual risks as threats keep changing. So, there is no absolute security. When it comes to changing threats, I tend to think of increasing threat velocity, this increasing threat velocity has several dimensions:

- More and more vulnerabilities being discovered, so more attacks,
  - Product Vulnerabilities
  - System Misconfigurations
  - Insider Threats
  - Social Engineering
- Evolving set of actors (bad guys)
- Attacks happening sooner and faster
- Easy to carry out attacks

Also, the attackers have some advantages over the defenders

- Defender must defend all points. Attacker can choose the weakest point
- Defender can defend only against known attacks. Attacker can probe for unknown vulnerabilities
- Defender must be constantly vigilant. Attacker can strike at will
- Defender play by the rules, whereas attackers can play “dirty”.

There is also the problem of attribution when it comes to attacks Attribution.

Who is attacking” and the “Why”?

This is a difficult problem due to several reasons:

- Open and unauthenticated nature of the Internet
- Information relating to source may not exist or be inaccurate
- People with relevant data may be reluctant to share, e.g., legal constraints across boundaries
- Even when data is shared, may still be hard to reach consensus on what the data means.

Hence when it comes to policy settings, it is more about probabilities and thresholds.

What is the right probability threshold? What is the right tolerance level for harm? And what action is proportionate?

Cyber and Disruptive Technologies

I would like to focus on certain technologies where cyber plays a key role, and which are relevant for AUKUS.

Critical Infrastructures

These are assets seen as being most crucial to the nation, by virtue of their interdependencies across sectors, and the potential for cascading consequences to other critical infrastructure assets and sectors, if disrupted.

The Legislation itself has several security obligations. For instance, certain organisations are required to report cyber incidents to the Australian Cyber Security Centre, that impact the delivery of the essential services.

The Enhanced Cyber Security Obligations include:

- developing cyber security incident response plans to prepare for a cyber security incident
- undertaking cyber security exercises to build cyber preparedness
- undertaking vulnerability assessments to identify vulnerabilities for remediation
- providing system information to develop and maintain a near-real time threat picture.

5G Infrastructures

5G networks are much more than just faster speeds. They introduce greater capacity, reduced latency, and more flexible service delivery. They enable organisations to provide richer content, more real-time transactions, and better user experiences.

First, 5G can help to create powerful edge-based networks that can share and process information locally as well as with cloud resources. For instance, IoT devices can track other devices and users, monitor inventory, gather user and device information, and provide real-time data.

Such connected environments have serious consequences for cyber security. The biggest challenge is the dramatic growth of the attack surface due to the rapid expansion of IoT devices and edge-based computing. With billions of IoT devices interconnected across a meshed edge environment, any device can become the weakest link in the security chain and expose the entire enterprise to risk.

AI and Cyber

AI technologies impact both sides of the coin, so to speak, when it comes to cyber. That is, both attackers and defenders can benefit from AI technologies.

Incidentally when I say AI, I want to focus here only on machine learning, which is probably the most relevant technology of AI for our purposes.

In a nutshell, machine learning algorithm has 3 main parts:

1. A Decision Process: Based on some input data, algorithm will produce an estimate about a pattern in the data: often a prediction or a classification.
2. An Error Function: An error function serves to evaluate the prediction of the model. If there are known examples, an error function can help to assess the accuracy of the model.
3. A Model Optimization Process: If the model can fit better to the data points in the training set, then weights in the model are adjusted to reduce the discrepancy between the known example and the model estimate. The algorithm will repeat this evaluate and optimize process, updating weights autonomously until a threshold of accuracy has been met.

One key point with machine learning systems is that they have the capacity to learn and modify their own behaviour to achieve their objectives.

We have different types of learning, a common one is supervised learning. Here we have data that have been labelled, such as bad data and good data, and the algorithm learns using these known labelled data. Once the algorithm has learned sufficiently, we can use the algorithm on test data.

In my view, at present, defence is in a weaker position than offense due to the various factors that I alluded to earlier. Hence the help that AI can provide to improve the defence

capabilities will be useful for correcting some of the imbalance between the attackers and defenders.

Another important area is that adversarial learning. This is about finding the vulnerabilities in the machine learning algorithms themselves. Attackers use these techniques to cheat and attack machine learning algorithms.

So, we need to design trustworthy machine learning algorithms that can withstand such attacks from the attackers.

We also need to have a better understanding the decisions made by machine learning algorithms, that is, why a particular decision has been made and not just what the decision is.

Autonomous Systems and Cyber

An autonomous system is a collection of distributed entities or agents, interacting and collaborating with each other, carrying out a multitude of tasks, to realize the overall system goals.

This can be, for instance, a group of drones interacting with each other in a dynamic and contested environment. Autonomy can be partial in that there can be some degree of human involvement.

These autonomous agents need security mechanisms to:

- detect and counteract attacks,
- to determine which agents are friends or which ones are enemies, so that they can collaborate with trustworthy agents, and
- to take decisions based on data that is accurate, as well as having reliable mechanisms to evaluate the quality and consequences of their decisions and actions, and learn from experience.

Space and Cyber

The final area of critical technologies that I want to mention about is that of space, which I believe is important for AUKUS from cyber perspective

With the increasing commercialization and militarization of the space sector, the attractiveness of space as a target for attacks will only grow in the future.

Most of the world's terrestrial critical infrastructures – communications, financial services, transport, logistics, weather monitoring etc. - are intrinsically dependent on space infrastructures. So, protecting space assets is critical.

Space systems typically consist of 3 segments, namely the space segment (with satellites and space objects), the ground segment (with all its command control and management as well as user and customer networks receiving data and services) and the link segment that connects the two.

All these segments are exposed to a range of cyber threats.

Another major area of concern is the supply chain vulnerabilities. The specialised components needed for space assets are not all developed by a single manufacturer.

In fact, to keep the costs down, space organisations often purchase components from catalogues of approved vendors around the world. The approval process for these vendors does not necessarily include cyber security vetting standards.

When a space organisation purchases a component from a vendor, for instance, it has little control over the code written by a software developer of that component. This lack of insight introduces considerable cyber security risk.

This makes space assets difficult, if not impossible, to patch for security flaws, when they are discovered.

Then there are the new emerging space services. For instance, the AWS Ground Station is a fully managed service that allows users to control satellite communications, process data, and carry out operations from their desktops and laptops, without requiring the traditional ground station infrastructure (such as from a space agency).

This implies that such services can be accessed by users from their desktops or laptops, from anywhere from the world. This introduces several security issues such as controlling actions from malicious users and ensuring malicious payload is not uploaded infecting space systems, as well as preventing denial of service attacks.

Another emerging technology is the softwarization of space systems. On the one hand, these technologies will make space systems more flexible, allowing introduction of new functionalities as well as dynamic configuration of satellite functions to meet changes in demand. On the other hand, it also introduces new security challenges. When the new functionalities and services are introduced dynamically there is a need to ensure that they are secure and trustworthy and that sophisticated security attacks can be prevented.

It is clear that mitigating cyber threats in space require not only technological solutions but also policy solutions that can guide the technology efforts.

Defence image

For instance, with the increasing reliance of the space sector on commercial technologies and the use of commercial off the shelf components, it is critical that polices should be established to enforce strict cyber security requirements for all components of space systems and their supply chains.

Cyber security skills are another important piece in the policy framework. A major challenge in securing space systems is the "systems of systems" aspects, requiring a deep understanding of how such systems work and the various threats and opportunities for the attackers to disrupt them. With space systems, expertise in both system infrastructures such as servers, networks, and systems as well as knowledge of specialised space infrastructures such as ground control systems and satellites are needed. The policy framework should identify specific steps in developing professionals who have capabilities and expertise in both these areas.

AUKUS and Other Initiatives

It is estimated that there are some 3 million cyber security professionals will be needed throughout the world by the late 2020s. In Australia, this figure is around 25000 over the next few years, whereas in the US it is over 800,000.

So, there is a great opportunity to enhance cooperation in the cyber skills area and synchronize some of the activities in education and research in cyber security between the QUAD and the AUKUS initiatives. For instance, mutual recognition of some specific educational programs in cyber security.

In fact, mutual recognition of security assessments like IRAP (Infosec Registered Assessors Program) and security standards for procurement of software, across AUKUS and QUAD countries, will enable companies that pass security assessments in one country to sell into the partners' markets.

On the technology side, there can be some low-hanging fruits such as agreements on the next stages of 5G/6G. Another area which comes to my mind is in the establishment of a framework for identifying and fact-checking monitoring system targeted at cyber threats, which would be beneficial for both QUAD and AUKUS.

Also establishing government agreements between the partners in the tracking down of cyber criminals, potentially putting pressure on financial entities enabling them to operate, as well enabling increased transparency.

This can also help with attribution of activities of malicious actors and cyber-related sanctions.

Then there is the conducting of joint cyber exercises with the partners from the QUAD and AUKUS to improve interoperability and resilience capabilities.

Another area that should be explored is in the context of foreign policy, related to foreign aid. There can be coordination of policies with respect to foreign aid resources in cyber and technology capacity building in the region—a dual benefit for the economies and resilience of our regional partners, as well as our own security.

Conclusion

In conclusion, cyber poses global challenges, which can only be met through close alignment and co-operation amongst major powers. Initiatives such as AUKUS and QUAD provide ideal channels for Australia to enhance cooperation and collaboration in cyber, in particular, in enhancing its cyber security capabilities through sharing of expertise, and investment in skills, enabling the partners to develop and exchange advanced technologies and strengthen their interoperability and resilience.

For AUKUS to be successful, I believe it should play a significant role in areas such as secure supply chain and interoperable security standards, which are particularly relevant (and require urgent consideration) for cyber technologies in defence and space.

Furthermore, I believe AUKUS should engage with the industry and bring them along in shaping the AUKUS initiative. This will be critical for its success. Increasingly, we are seeing an increasing focus on cyber security in the boardrooms of US, UK, and Australian organisations in both public and private sectors. Alliances like AUKUS can have a positive influence on such boardrooms, when every executive team will need to assess cyber risk and understand the mitigation opportunities afforded by technologies such as AI, autonomous and cloud systems.

Vijay Varadharajan
The University of Newcastle
vijay.varadharajan@newcastle.edu.au

images Adobe stock.