Australia-China Relations Institute
澳中关系研究院

Transcript

Cyber impacts on the US/PRC military balance

Speakers: Professor Greg Austin, Adjunct Professor, UTS:ACRI; China cyber and strategic policy expert

Ms Caitríona Heinl, Executive Director, Azure Forum for Contemporary Security Strategy

Moderator: Dr Marina Yue Zhang, Associate Professor – Research, UTS:ACRI

July 6 2023

Online

E&OE | Check against delivery

Dr Marina Zhang:

Good evening, ladies and gentlemen. My name is Marina Zhang and I will be the moderator of tonight's webinar. Before we begin the proceedings and on behalf of all those present, I would like to acknowledge that Ngunnawal people as traditional custodians of the land from which I'm hosting today's webinar and recognise any other people or families with connections to the lands of the ACT and region. Greg and I are both in Canberra. I would also like to pay respects to the Elders both past and the present, acknowledging them as the traditional custodians of knowledge of this land.

This session is recorded. We record audio, video and screenshots by our presenters, but we will not record any video or audio input from the audience. Welcome to all UTS students, staff, or friends of ACRI and UTS.

Australia-China Relations Institute known as ACRI at UTS is an independent non-partisan research institute established in 2014. For those who don't know ACRI that well, we are Australia's first and only research institute devoted to studying the relationship between Australia and China. UTS:ACRI seeks to inform all relevant stakeholders about Australia's engagement with China through research, analysis and dialogue grounded in scholarly rigour.

In the evolving world of today, the room of warfare is not confined to the traditional battlefields anymore. Instead, it has expanded into the cyberspace. Cybersecurity therefore is no longer an option. It's a strategic imperative, particularly as the power dynamics between nations like the United States and China unfold in this space. Understanding the battleground presents enormous challenges. It's not an open field where you can see how your opponents or your enemies charge. It's a shadow realm of codes, algorithms and hidden vulnerabilities.

In international relations, nations often opt for deterrence capabilities operating under the principle that best defence is a good offence. However, it is important to know that in cyber warfare, the advantage often lies with the attacker, at least initially, as it's generally easier to exploit vulnerabilities in a system than it is to defend against every potential threat.

The implications of such threats are far-reaching. So here we stand at the intersection of digital technology, security and international power dynamics. The cyber battlefield of the future will require all nations to protect critical infrastructure, safeguard intelligence systems and secure national interests.

So joining me today on the panel are Professor Greg Austin from Canberra and Ms Caitríona Heinl from Ireland – I hope I pronounced your Irish name right.

Greg Austin is an Adjunct Professor at UTS:ACRI. Greg is recognised internationally as a leading researcher on China's cyber policy with two books and numerous articles on that subject since 2014, including work on Australia-China cyber relations. He has also published on China's strategic policy more broadly since 1997 – that's very early – most notably in Taiwan Strait security affairs, Japan-China relations, and China's maritime frontier. He has held senior positions in academia, think tanks and NGOs [non-government organisations] in both Europe and Australia.

Caitríona Heinl is Executive Director at the Azure Forum for Contemporary Security Strategy. Caitríona has over 10 years' experience within applied policy research, strategic advisory and capacity building environments, specialising in international security with focus on conflict prevention strategies related to international cybersecurity policy, strategic technologies, regional security architectures. She recently served on the Irish Government's Commission on the Defence Forces.

A bit about myself. I'm an Associate Professor here at ACRI. Before this position, I worked for UNSW and [University of New South Wales] Tsinghua University. My research stands on the intersections between technology innovation and national securities. I focus on industries such as semiconductors, biopharmaceuticals, clean energy transition and cyber orders.

Let's welcome Greg and Caitríona. They will take 10 minutes each to share their insights into cyber capability between the United States and China. Greg will cover the US military cyber capability in the case of cyber war with China and Caitríona will talk about the current state of play and near future for maintaining stability in the US-China power balance in relation to military cyber capability. Without further ado, let's welcome Greg and Caitríona.

Last thing, if you have any questions, you are welcome to ask the panel after the presentations. Well actually, you can submit your questions where the Q&A tab at the bottom of your screen.

Greg, you are the first to present. Let's welcome Greg.

Professor Greg Austin:

Well, thank you very much, Marina, am I coming through loud and clear?

Dr Marina Zhang:

Loud and clear. It's your go.

Professor Greg Austin:

Ladies and gentlemen, it's a great pleasure to be here and thank you for joining. Look forward to discussing this rather complex subject in a very short amount of time. So I'm going to be giving you what's really a 10-minute thesis about very complex issues.

My judgments in this presentation are quite firm, so I have high confidence that based on significant research by colleagues and by myself and in fact by teams of colleagues, that the judgments in this presentation are heading in the right direction. There's no time to present a detailed justification, so I'd be happy to discuss offline with anyone after the meeting at any point in the coming weeks or months about the judgments. The work here concentrates – so the presentation concentrates on cyber – but we've done some equivalent work on electromagnetic spectrum and outer space, which helps reinforce the judgments I'm making tonight about cyber.

So, as a bit of a teaser and a bit of a preview to the presentation, I'd just like to reflect a little bit on the role of the United States Navy in the Russian war on Ukraine. So no ships, but the Navy has been fighting in Kyiv. Navy personnel have been in Kyiv since at least December 2021, engaging with Russian military capabilities, of course in cyberspace.

I'm mentioning this because this is a really good example of the sorts of changes that are upon us in understanding the relative military capabilities of different countries. And certainly a sign of the times. The US government or US cyber command assesses that the team they sent to Kyiv, including naval personnel, not exclusively Navy, but the team they sent to Kyiv helped defeat what otherwise would've been crippling cyber attacks by Russia and might have turned the outcome of the battle for Kyiv. So cyber capabilities can have a decisive impact on war, we've seen that. Perhaps the debate is just how much.

The United States believes firmly that it can fight and win in cyberspace. Now of course that means many different things, many different levels of fighting from tactical through operational to strategic. But just to give a bit of a flavour of this sentiment, I've pulled out three quotations. The first from 2009, the second from 2013, and the third from 2020. So the first mentions the value to the United States of global strike, which can be achieved in milliseconds. The second comes from US Navy training video, which says cyberspace is where the battles of the future will be won or lost. And in 2020, the former commander of the US Indo-Pacific Command said that the United States was aiming for the penetration and then disintegration of an adversary's systems and decision-making, thereby defeating their offensive capability. And this is about cyber capability disintegrating the adversary systems, paralysing their decision making and defeating their kinetic offensive capability. This is a pretty strong statement, but it's an important reference to what the United States believes it can achieve.

So, how do we assess relative cyber capability? As Marina correctly said, you can't see it in the same way that you can see military ships and aircraft. And traditionally relative military balances were assessed around comparing like with like, how many aircraft carriers does one country have compared with how many aircraft carriers the other side has, how many destroyers, how many fighter aircraft, and the like. Well, that was pretty inappropriate even when it was being done. And eventually there's been a shift to an understanding that a real military balance of power or balance of capabilities can only be understood if we compare ships with anti-ship systems, ships on the one side with the anti-ship systems of the adversary, aircraft on one side with the anti-air system to the adversary. And the same with missiles and missile defence.

So, if we're looking to understand the military balance of power between two countries, we really want to understand or want to compare the cyber offensive capabilities of one country with the cyber defence capabilities of the other. And as I mentioned, and really what underpins very much my judgment about the superior military cyber capabilities of the United States is that China has very weak cyber defences. And you have to look long and hard before you can find any assessments of Chinese military cyber defences or even of China's cyber defences, period. Everyone seems to want to focus on how wonderful their cyber espionage has been and it has been, but there's very little attention paid to China's cyber defence.

So, what are we looking at when we are looking at military cyber dominance? And we're really looking at dominance in intelligence and the overall intelligence capabilities of a country like the United States and

its allies on the one hand versus the overall military intelligence capabilities of a country like China is an important factor in framing of my judgment that the United States has a considerable and clear superiority over China in cyberspace.

The cyber intelligence is delivered not only for the purposes of broad national security intelligence, but it is also delivered for the purpose of conducting cyber defensive operations and cyber offensive operations. So military cyber capability is predominantly intelligence capability that's exploited by others. But we also look at the capacity of one country or another for systems destruction warfare, especially with a focus on critical information infrastructure. And we also look at the comparison of the industrial strengths and workforce. But we also have to look a little bit more deeply into the armed forces at things like officer trust in cyber capabilities for war fighting and in the political will of leaders to fight in cyberspace. They're very important considerations.

So, I've got a list of 10 military cyber missions on the screen. I'd like you to contemplate what the impact of a cyber campaign by a powerful country would look like in war if each of these missions were executed at scale. So what would war look like if each of these cyber missions were executed at scale? I'd just like to flag a couple of them for a little bit more reflection as I go through the list. What does punishment look like in cyberspace at scale? What does cyber degradation look like at scale? What does cyber decapitation look like at scale, and so on. Mass psychological operations, information theft, every single war plan that a foreign country has is at some point, or usually at some point, put into cyberspace and therefore susceptible to interception. But more importantly, countries have to be able to conduct kinetic campaigns to seize the information terrain. So, it's highly complex, there are many different dimensions, and if delivered at scale can be overpowering.

So, if we want to assess a relative order of battle, relative military capability, we have to assess the cyber missions and the cyber organisations; we have to review the degree of combat testing, the type of exercises and training that are held; we have to have knowledge of the flexibility that the armed forces can demonstrate in accessing cyber resources for offense and defence; and we have to understand what the combat cyber intelligence capacities of adverse repairs are.

But to go back to the point I mentioned about the officer trust in cyber warfare operations, we have to understand the social decision structures and biases in the armed forces. This is a dimension that is almost never analysed in public discussions.

So, the Russia-Ukraine war, what does it tell us? Well, the war by Russia on Ukraine has seen the largest, most damaging cyber attacks in history, the largest and most damaging cyber attacks in history. The war has also seen the most wonderful and inspirational cyber defence in history in terms of scale. And it's not easy to get a sense of the scale of the attack or scale of the defence for most 10 page academic journals that you find or even in longer books necessarily. But it's really important to understand that this is the largest cyber war in history. So we can learn lessons from it.

We should understand that Russian cyber forces have repeatedly been on the offensive and they've been consistently losing. So this bears out a judgment that the IISS [International Institute for Strategic Studies] made just before – on the eve of the invasion, we published an assessment suggesting that Russian cyber forces were more or less in that position.

And finally, the war has demonstrated that with this war, which is between Russia on the one hand and Ukraine and its Five Eyes allies on the other, has proven, to my mind, that the cyber military balance between Russia on the one hand and the US and its allies on the other, is heavily in the favour of the United States and its allies.

So, turning to the China case. For similar reasons, we can make a judgment that the military balance between the US and its Five Eyes partners on the one hand versus China, is very heavily in favour of the US and its Five Eyes allies.

The challenge is now how to exploit that in kinetic, political and psychological battles, and how to assess the likely outcome of those. But we have to understand, above all else, that the key to success in exploiting that advantage by the United States and its Five Eyes allies, will be cyber intelligence and cyber daring.

So, the implications: Very quickly, China knows that it is outgunned in cyber capability by a global alliance. And for that reason it is deterred from a decision for large scale military confrontation with allies over Taiwan.

Now it's a big judgment, but I'm convinced that the cyber military capabilities of the US and its allies are so clearly in favour of them that China is deterred from a decision for large-scale war.

So, that leaves us in a very interesting situation. And as my colleague, Caitríona, will now take us forward, it means that cyber insecurity, and insecurity in general, between the United States and China is intensifying.

Thank you ladies and gentlemen.

Dr Marina Zhang:

Thank you, Greg.

Caitríona, it's up to you.

Ms Caitríona Heinl:

Great.

I've just unmuted, so let me know if you can't or can hear me. Marina, you can hear me?

Dr Marina Zhang:

Yes, we can hear you. Go ahead.

Ms Caitríona Heinl:

Wonderful. Great. Thanks Marina. Thanks Greg.

So, good evening to those colleagues in Australia. It's morning here, so forgive me if I refer to morning and evening or get them confused.

I'm also delighted to be here and particularly delighted to have time to hear Professor Greg Austin's analyses on these questions.

So, like Greg just explained, the angle where I think I can add some value to the discussion this morning is just considering some of the developments surrounding the state of play and near future for maintaining stability in the US-China power balance, in terms of the impact of military cyber capability.

So, by now, generally speaking, just as a framing point, militaries, including in the US and China, generally have a far more mature understanding of the nature of cyber capability in military terms. Sorry, what we're speaking to really is in terms of strategy, technological capability and structures.

So, for instance – and I love Greg's analysis in terms of where we are today – what we're seeing now is more a mature military cyber structures that are beginning to bake in the practical interconnections with military intel, counter hybrid warfare, emerging and disruptive technologies and defence research and innovation.

So, the bottom line upfront that I want bring the table this morning, that all said, risk reduction mechanisms associated with cyber, digital and emerging strategic technologies must still be developed. So these are not nearly as robust as they should be.

And in terms of the US-China military cyber stability aspects specifically, it's really still the case that there are insufficient confidence building and transparency measures such as mill-to-mill engagement, dialogue and crisis communication procedures in order to prevent misunderstandings or escalation.

And now, and this is where I really want to focus my attention, that particular situation – which has been the case really for quite some time, is even more exacerbated by a number of new developments that I, in my opinion, are potentially even more destabilising at what we view as a time of fierce competition between the two powers.

We have 10 minutes, so I'm going to run through as quickly as I can at some of the types of developments that I think need a little bit more of our attention if we don't want to find ourselves in crisis, so to speak. So remaining in that state of competition [inaudible].

So, first, broadly speaking, and most of you on the call will understand this piece in terms of the geo-strategic relationship, but the negative impact of the fraying strategic relationship naturally has to be considered. So relations are at their lowest really since the Cold War. Geo-strategic tensions are far higher than they were, say a decade ago, when some of us were conducting these types of similar analyses with respect to military cyber capability.

And so the potential for crisis or talk of war has become somewhat higher. Prior analyses often considered, including my own, US-China cyber questions through the prism of bilateral and regional stability. But it's clear that this is a global stability question now concerning not just those nations in the Asia-Pacific region, but all countries across the globe.

Taiwan – and of course Greg has spoken to some of his analyses vis-à-vis Taiwan – this was naturally always part of analysis in this space, but there seems to certainly be heightened consciousness, especially since the invasion of Ukraine. And so together with the return of great power conflict, the technologies that are being used are changing. Again, in my opinion, but also we'll see this in some of the literature, changing faster than we can analyse.

And so that brings me to – I'm going to delve in a bit more deeply into some of the types of areas of new developments that we need to spend time on. The misaligned perceptions between the US and China seem to still be continuing, together with uncertainty on what we would call military cyber stability.

So in relation specifically to communication channels, it goes without saying that COVID impacted dialogue, including amongst some of the informal expert networks. There's no Track One dialogue. And generally speaking, formal communication channels are not in use.

So, just in very broad terms, what this means is that it's naturally impacting the ability for these two powers to understand each other's way of thinking, intentions, but also importantly the perceptions of each other to activity.

So, to give you two very quick examples, currently there is a sense of misperceptions about the types of signals or how ongoing cyber activity is actually perceived. So this sense of perception of cyber activity and signals are still being figured out.

So, my conclusion with respect to that piece is that there really is still a lot of work to do for us to clarify how to manage escalation as both powers are still figuring out what each other finds tolerable, but also what theories are palatable.

And then the third area that I think we need to consider in this regard when we talk about military cyber capability is the fact that malicious cyber enabled information activity and high levels of cyber espionage activity have also become destabilising in this space. So, it goes without saying there's a general acknowledgement, even up to the UN [United Nations] level, that cyber enabled information activity is undermining trust and it's possibly escalatory.

And so when you combine this with what I would describe as the already blurred lines between unregulated state cyber espionage activity and state use of offensive or defensive cyber tools, this could become even more blurred and possibly more destabilising in ways that we have not necessarily seen before.

And so, the conclusion with respect to this newer, more recent type of cyber activity is that, if we consider unprecedented high levels of cyber enabled espionage combined with hybrid cyber-related activity below the threshold, this is all taking place alongside trade warfare dynamics and downward spiraling geo-economics trends, such as technological decoupling.

So, just on that last point, when we talk about stability, it's not quite clear yet just how de-risking or technological decoupling, how they might impact long-term stability. So I still think there's a question mark surrounding that.

The next area in terms of broad trend areas that are new developments that I think we have to consider when we talk about the power balance and military cyber capability is that of the relationship or the nexus between cyber capability and new technologies and how the nexus is increasing, but also how they're becoming more increasingly interconnected as we go forward in the next few years.

So, that particular space is certainly, I'm nearly convinced, bringing about technological and analytical uncertainty. So there's a lot of questions and very few answers.

Just broadly speaking, as a framing, we know that there are a number of new technologies that can or possibly could, bring about a disruption or a paradigm shift for military affairs. And some analyses, if you bear with me, find that the implications for war fighting and strategic stability are difficult, and here I'm paraphrasing, if not impossible, to predict at the moment. And so the conclusion in this regard is that these types of gaps and strategic understanding and predictability could potentially bring about additional destabilising factors when we start talking about these interconnections between new technologies, cyber capability, and so forth.

So, a very minor or basic example there would be an emerging and disruptive technology like AI [artificial intelligence], or the military use of these types of new technologies, can assist cyber operations, but also we find ourselves in a situation where decision times are reduced.

I see Marina, I'm going to conclude now in a minute or two. Just another aspect that I think is relatively novel, and I think it was mentioned in one of the bullet points by Greg, is the dual use aspects of these technologies, which means that synergy, they're being promoted between the civilian and defence research and innovation spheres.

So, this again is an important factor for us to bear in mind when we're talking about the nature of future military cyber and technological capability and how this was traditionally the preserve of military. But this newer type of innovation is certainly, as seen or regarded, to be mostly civilian sector driven.

I think on AI [artificial intelligence] specifically, I think those interconnections with military cyber capability that experts are considering, one key question is what is the impact of AI systems on strategic stability with nuclear balance when we start talking about worries about how to control escalation or misperception?

Another last aspect there, and I'll close off on the EDTs piece, is with respect to evolving cyber capability. How does the cyber posture impact nuclear stability where Chinese nuclear capability is growing?

And so my last concluding remarks, I think I have my last minute or so with Marina, is just very broadly speaking, we've known for some time that third party actors do add complexity to the military balance. So, while it's been in the literature for some time, there's generally a sense that there is more evidence of a growing number of non-state actors, either expressing an interest in or actively using cyber-related capabilities, that were traditionally preserved of states.

And so again, for both of these powers, like the United States and China, how should they be managing non-state actors' activity so that it's not destabilising? Greg spoke to some of the lessons already coming out of Ukraine. We saw there the involvement of third party non-state actors in a time of conflict. And so just to conclude on Ukraine, I think it's clear, and I know we'll get to speak in more detail about Greg's presentation, but just broadly speaking, it's clear that some of the observations and lessons from the conflict will change strategy and long-term thinking on military cyber stability. So what we're seeing is this move away from the abstract to practice. So what works and what doesn't work will be analysed. It's probably safe to say, for example, that Chinese actors would naturally try to understand US thinking from case studies like responses to the Ukraine invasion.

I think, and I'm going to use a slightly different language to Greg, but I think it's speaking to a similar point, the conflict has also been showing the importance when we talk about capability of cyber defence capacities, that Ukraine has really been maturing since the last encouragement in 2014. I think this could potentially be rather relevant when we think broadly speaking, there is that sense that critical infrastructure vulnerabilities are sometimes understood to be rather high in the United States when we talk about civilian infrastructure at least.

And the very two last points vis-à-vis future conflict and this type of military cyber capability is Ukraine has clearly shown the importance and the decisiveness of close cooperation with the private sector. So what does that mean for these powers when we talk about military cyber capability for future conflict, but also it has shown the necessity of having cyber reserves for major cyber attacks. So again, how do we define and develop military cyber capability and what do these types of developments mean in that either traditional or non-traditional definition of capability?

So I'll stop there, and thank you for your patience, Marina. Thank you.

Dr Marina Zhang:

Thank you, Caitríona, for your analysis. You got two minutes to comment on what Greg said in his presentation. So you covered a little bit, but if you can elaborate a little bit more, that would be great.

Ms Caitríona Heinl:

Certainly. Great. Okay. Sorry, I thought you were moving across to Greg first, but that's no problem at all.

Just yeah, certainly a few items actually that I would be in agreement really with Greg about. On Ukraine particularly, I think that focus in one of Greg's bullet points on the January 2022 focus on cyber defence, to mitigate possible crippling attacks I think is one of the key lessons coming out of this current conflict.

I think just to throw a little bit, and I know Greg, I'm sure you're even aware of this yourself, but there has been some interesting material either in speaking engagements or in literature from Professor Lawrence Reedman, or Freedman rather. Some of his recent thinking is that cyber has not been as decisive as the literature or the analysts would've kind of argued to date in terms of future warfare. And so it's really good to hear Greg's analysis based on all the research that you've been doing over the past few years with your teams, Greg, surrounding cyberspace operations as in fact decisive. So I think that would be interesting to hear a bit more about what you think about as Sir Lawrence's thoughts in that regard.

And then two or three other points that came to mind. Again, speaking to that cyber defence, cyber resilience piece, it certainly seems to be the case that one of the lessons from Ukraine, and I know it's going to take many years by the way to really understand this and unpack it carefully, it's quite recent, so I'm also sometimes hesitant to draw conclusions that are too rigid. But Greg spoke to this need to understand and compare cyber penetration with cyber defence. So I think that certainly is the case. What I would add to that is that in times of conflict or times of war, I guess we're not just talking about military targets in times of conflict, but civilian critical infrastructure too. So what does that mean when we talk about cyber vulnerabilities and cyber defence?

Yeah, I think it goes without saying that most people in the field vis-à-vis the commentary surrounding military cyber intel and the fact that that amounts to nearly 90 percent so to speak, of what we define as military cyber capability, I think certainly in the US-China example, most would agree with that, but I'm not sure the rest of the world has necessarily caught up with that in terms of their own capability or structures. So I do think it was great to hear that from Greg.

Dr Marina Zhang:

I think you might just keep your questions for later during our discussion.

So Greg, I would like you to just using two minutes to comment on Caitríona's analysis.

Professor Greg Austin:

Sure.

I think that Caitriona has a very strong advantage over me in that she's had more contact with specialists from China in the recent past and from the United States to understand really how these dynamics are playing out. It would be interesting to contemplate really just how sensitive the Chinese have become or how insecure they've become, what we've seen in Washington. So, Caitriona is exactly right in pointing to the trend

of increasing insecurity, that increasing insecurity in Washington has been profound, but there's been less mapping of the similar trend in China. So, it's a bit hard to know where to start to look.

And if we could allow Caitríona some comeback on this, I think it'd be really good to understand what sense she has of what is the trend of insecurity in China? Is it just more insecurity? Or in the Chinese reaction to US export controls ever tightening, China's introduced its own export controls, so we can see a sense of insecurity there on the Chinese side. But compared say with the last live Track Two discussions that Caitriona might have been involved in several years ago and recent discussions, what's that trend of insecurity look like? I think it'd be really interesting to hear on the Chinese side.

Dr Marina Zhang:

Right. I think before we discuss, we have one question here which is addressed to Greg. I want you to maybe elaborate your thought on that question.

So, question from Fabien: 'Do you think that the RAND assessment in 2017 claiming that the US has an advantage over PLA cyber capabilities, Taiwan scenario, is still valid?'

Professor Greg Austin:

Yeah, thanks for that question, Fabien.

I do, but let's add a little bit of background to that. So, since 2017, a number of analysts in the United States and Australia have pointed out that China has embarked on a massive ship-building and ship-launching program. So, some people say, for example, that between 2000 and – I think it's between 2000 – oh no, it was around about the same time in fact, that they point to the very large number of ships that China has launched, I think, in the period up to 2018 compared with what the United States has launched. So, we do have to take that into account. But we also have to do the counting ourselves. And many of those alarmist reports about the so-called massive advantage that the PLA [People's Liberation Army] Navy has got over the United States Navy in ship numbers is not really what they say it is. But more importantly, the ship numbers like/unlike is not a good way of understanding the relative balance of power. I think what we've seen in respect of United States balance of power relative to China over Taiwan is a very substantial stiffening of resolve on the part of the United States to military defence of Taiwan. We've seen a substantial increase in the preparedness of the United States to conduct operations around Taiwan in cyberspace as in elsewhere. Other domains, we've seen Japan engage on its own military buildup. So I think that there's all sorts of reasons to think that the RAND assessment of 2017 still holds good.

Thank you.

Dr Marina Zhang:

Thank you, Greg.

So I think the three of us can engage in the discussion. How about I start with a question for you both because you both talk about it, but not in great detail, from different angles. I just try to make sense – when you're talking about military cyber capabilities because this is a highly classified area and we really as outsiders don't know the detail or inside stories.

So Greg, you talk about cyber capability largely in the area of intelligence. And Caitríona, you talk about, well actually it's a sort of a blurring area how to define cyber capabilities because capabilities may include, well, for example, resources from civilian or including strategic capabilities because not only just your comeback

capability can determine the win or lose in the battlefield, even in the cyberspace. So how do you both explain this? Elaborate a little bit more on this capability definition.

Professor Greg Austin:

Well, let me go first, if I may.

Dr Marina Zhang:

Sure.

Professor Greg Austin:

Now, a very tough question, but we are actually aided in a number of ways.

So if our basic proposition about net cyber military capability is to assess the defensive capabilities of one side versus the offensive capabilities of the other side, we can see in the public domain, evidence that China has weak cyber defences and that China has not conducted the range of offensive cyber operations, not including espionage. China has not conducted the range of offensive cyber operations that Russia has. When it comes to comparing Chinese operations towards the United States in terms of offensive cyber operations, the evidence is less clear, but we know that the United States has been authorised by the president of the United States to conduct offensive cyber operations in several crises situations beginning in 1999.

We know that the US Naval Cyber Command has 16,000 people available. We know that the Australian Navy in its entirety has about 16,000 people available. We know that the United States military cyber effort has 238,000 people available: military, civilian, and contractors. We know how much the United States spends on its cyber capability in broad terms and on specific capabilities. We don't have the same detail for China, but we have convincing assessments out of China that the country's cybersecurity is weak. And why is that? There's all sorts of collateral for that. The workforce is relatively underdeveloped. We can study in the public domain the quality of the courses that are taught at all Chinese universities, except perhaps the most secret. But certainly in the Chinese Information Engineering University, we can see online what courses are taught. We know how many people are coming online into those courses. For example, in 2019, China's PLA Information Engineering University started its first course in artificial intelligence at undergraduate level and had 30 people come into it.

So, we do have rather interesting, reliable public source information on a lot of these things, but it does take close examination to get to the bottom of it. But most importantly, we can look at what the Chinese are saying about their own capabilities. There's enough in the public domain to give us a pretty good impression. And if you read United States documents carefully, at the end of the day they reveal a comfortable assessment that the United States maintains clear superiority and they provide all sorts of evidence of that in different ways.

Thank you.

Dr Marina Zhang:

Caitríona, your comment on this issue?

Ms Caitríona Heinl:

Yeah, great. Yeah, I tend to completely understand the direction of analysis from Greg.

I think what I would draw out in terms of how we understand this type of capability if I understood your question correctly, is I would kind of speak to the types of points I raised in the opening remarks in terms of a broader composition of how we traditionally define or understand military cyber capability. And so in that regard, I think of course it goes without saying the military intelligence piece is kind of a key underpinning aspect of this. But also now as we're seeing, and we'll see much more of this actually in the next few years, just that link with the development and use of all sorts of new and emerging technology areas.

I think, again, moving away from a traditional understanding of the space, just what does it mean in terms of the private sector. Greg had on one of his slides, you might have seen it, he referenced corporations vis-à-vis what we're seeing in the Ukraine conflict. So again, how do you bring that into your understanding or composition of military cyber capability reservists? So again, we're not talking just about tools, we're talking also about the talent, the personnel, the people. So that kind of role of the reserves when push comes to shove. And if we were to find ourselves in a time of more.

And then the very last aspect in how we understand this space or the composition of it, I think again we're going to see more of the increasing importance of the role of the defence and technological industrial base going forward. So again, that's slightly different to the traditional domains that we might have been dealing with in the past. So that would be my very quick analysis to your question.

Dr Marina Zhang:

Thank you.

Coming to the second question. Responding to the point, Caitríona, you made in your analysis, you talk about increasing insecurity especially from China's side, this can trigger kind of a competition for more security. So this falls into this very classic trap, so-called security dilemma. Because we all operating in the dark, in the shady area, and we don't know what really the other party holds in terms of their capabilities. So, we therefore increase our capabilities and to deter the other party. So, this kind of competition, in your view, is increasing disability in the geopolitical landscape? So, I want you both to comment on this issue. Is this what's happening, or is this just our guessing?

Ms Caitríona Heinl:

I'll go first, Greg, because I think it speaks to the point you raised in your own question about my presentation.

And just to clarify, I would say, Marina, in terms of insecurity, I believe the insecurity is both from the United States and China. I don't think it's just China, and I just want to clarify that.

Dr Marina Zhang:

Thank you.

Ms Caitríona Heinl:

I also don't believe it's as shady, so to speak, as we might have spoken about 15 years ago or 10 years ago. So what I think will speak to your question and also Greg's remarks about how we understand maybe some of the perceptions or views on maybe Chinese thinking vis-à-vis insecurity, I kind of really have three or four overarching personal observations.

I think it all comes down to perception. So I think what's happening at the moment is how would a state like China understand US activity in a time of competition? I don't think the answers are there. I think there's a sense that this is still being figured out.

So, to give you an example, if that helps, if we talk about even US doctrine or even whether it's a theory like persistent engagement or defend forward, it's not only a case of, well, what US thinkers think about this doctrine and whether it's effective or not. It's actually how it's perceived. And it's the perception space where the insecurity and the instability can potentially arise. So if it's not perceived in the same manner, then obviously you're not, if there's two different maps of the world. And I think this is the space I would imagine we all find ourselves in now in terms of preventing escalation or misperceptions, is figuring out or at least clarifying and helping each other understand respective perceptions.

And another, I'll stop here, I think some practical ways also of providing clarification, if I were sitting in China, for example, is how the US responds. We spoke a lot about Ukraine this morning, that's fine. But how the US or even other parties would respond to other cyber scenarios in other parts of the world, I think would also provide kind of practical case studies or scenarios that Chinese thinkers would probably apply their mind to in terms of understanding the space and informing their own perceptions more clearly. So again, there's probably a signaling aspect there.

So, I hope that speaks to your question.

Dr Marina Zhang:

Sure. Definitely.

Greg, your comments?

Professor Greg Austin:

Yes. Well, as nervous and insecure as the Washington establishment has become about China, I would really like more evidence on what's going down in Beijing, in terms of how they really think about things.

We have some signals, so Xi Jinping said several years ago already that the country is facing, or the world is facing its most uncertain times for 100 years. So, that's a signal of higher degree of uncertainty.

But I think the Chinese uncertainty and insecurity is growing, especially in the face of the strengthening of the US and allied position in respect of Taiwan. The deterioration of Russia's position must be deeply alarming to China. The UK Armed Forces issued a statement recently saying that half of Russia's combat capability has been destroyed. Now, if that's true, what does China think about that?

And I think that what we see, a series of nervous reactions from China when they make a reaction about certain key developments. So when Starlink launched all those satellites to support Ukraine in 2022, Chinese PLA made a very nervous statement about how this was a threat to strategic stability. And we should note that in 2022, the United States launched more satellites than China has launched in its entire space program. So in one year, the United States launched more satellites than China has launched in its entire space program. The Chinese space capability is, according to an institute of the US, United States Air Force, decades behind that of the United States. Not a few years, not a decade, but decades behind that. And not everybody in the United States agrees with that. But as soon as China manages to make these great breakthroughs in space, about putting something on the dark side of the moon, at the same time, the United States is launching all of these satellites and making huge breakthroughs. China really doesn't have an immediate answer for this sort of stuff.

And in their statements about the industrial base, in their statements about the workforce and their statements about the state of cybersecurity, and in the nervousness of their reactions domestically to things like Hong Kong and Xinjiang, which are extreme in their orientation, in my view, it must reflect deep insecurities. But it really does deserve much closer study, and I haven't been studying it as closely as I would like to, to answer that question well.

Dr Marina Zhang:

All right. So before we answer another question from the audience, I just want to ask a hypothetical question. As I said at the beginning, so in cyber warfare, obviously attackers take a very obvious attackers' advantage.

So the question now is, given both parties, we all know the catastrophe a cyber attack can cause to a nation, destroying or stop the operations of critical infrastructures and so on, so who will do this first? Because the consequences is whoever does this attack first means it's walking away from the existing global order. So the question is, who will do this? We hope nobody will do it, but in your view, is that possible? Or what happen during the war?

Professor Greg Austin:

Go ahead, Caitríona.

Ms Caitríona Heinl:

I guess, just to the first part of Marina's question, funnily enough, I would potentially, maybe, not to be pedantic, but to kind of turn things on their head a little bit, I nearly would describe cyber defence as the advantage, rather than offensive capability, especially when we start talking about future platforms and that cyber penetration piece. So the ability to secure your future military platforms and so forth. So I personally feel that certainly that focus on defence and a possible shift away from thinking about deterrence, towards defence, is maybe one of the biggest shifts in thinking or lessons in the last two years or so.

At the last part of your question, maybe Greg can speak to. I wasn't quite sure what you meant about stepping away from the world order.

Professor Greg Austin:

Yeah, thanks. That's a really good question, Marina.

I think that Russia did it. So Russia tried to cripple Ukraine's critical infrastructure in the short-term. It wasn't a widespread catastrophic campaign, nor was it that well-planned. I think they thought they could get away with just a number of attacks. But Russia did it, and in that process, walked away from the world order. So you're quite right.

And so, even China today, and even the United States must pay attention to the voluntary norms developed by the United Nations, particularly the one about mutual assistance. So for example, once some countries of NATO saw what was happening in Ukraine, some of them, outside the Five Eyes alliance, came to Ukraine's defence. And I think the realisation globally, and especially in the corporate sector, that what Russia had done both in its aggression against Ukraine through the land invasion and the continuing missile attacks, but what Russia had done in cyberspace and continues to do is against world order. It's against the interests of leading corporations, and that's why Microsoft and Cisco and other companies are coming to the party. So yes, against world order.

Dr Marina Zhang:

I think we almost run out of time, but next question from Glenda.

I think, Greg, you are in the position to answer this question: 'How advanced is Australia's military cyber capacity and are we benefitting from US leadership in this area as a member of Five Eyes? Can they comment on how well placed Australia is and the implications of their assessments for Australia?'

Professor Greg Austin:

Yeah. Thanks, Marina. And thanks for the question, Glenda.

I think Australia is very well-placed in cyber military capability. It's been a slow process. So, in 2016, there was a bit of a kickstart from the Turnbull government, and they've been successive kickstarts with much more money.

What's really interesting is that the officer core is being brought along, not all of it yet. Defence education needs to travel a fairway yet, but Australia is certainly in the top 10 of cyber military powers, and it's only improving. What needs to happen in Australia is better alignment between the civil sector and cyber military policy, especially universities, and what the ADF [Australian Defence Force] might like to do. And the ADF needs a better reserve policy for cyber operations, I think.

Thanks.

Dr Marina Zhang:

Thank you, Greg.

Last question from Stephen. I think this is for Caitríona, or you are in a better position to answer this: 'Setting aside the imbalance in cyber power between China and the US, please can you comment a bit more on the likely impacts on our civilian sectors of the increasing grey zone competition between the two powers, and on the implications for our civil defence against these?' Didn't say in which country, but – ou got one minute.

Ms Caitríona Heinl:

Great. Gosh, I think you could go in a few directions, I think with that question.

I guess, if we're talking about peace time as opposed to during conflict, then certainly when it comes to grey zone, it's, I guess, the destabilising aspects of that. But also, well, certainly – I'm trying to think of the – 2015, 2016, there would've been a lot of focus on state-sponsored commercial espionage and what that means for the civilian sector, in terms of their IP theft for instance.

If you're talking about the civilian sector in terms of critical infrastructure, for example, then it goes without saying that there's a lot of peace time activity in those sectors. But I'd really prefer a more specific line of thinking from the question if we wanted to go a bit deeper. But I would certainly say there's a lot of activity in peace time at least. And of course, in wartime, it's possibly one of the target sectors to think about.

Dr Marina Zhang:

Thank you. I think we are out of time. Thank you, Greg and Caitríona, for sharing your insights into this very complex and very interesting, important topic.

And thank you everybody for attending tonight's webinar. I think we will send you an email, all attendees, reminding you – or send you a link, asking your feedback to today's webinar. We greatly appreciate your input, and your input will help us improve our future events like this.

And if you want to know more about Australia-China relations, please visit our website at australiachinarelations.org. And also, you can follow us on Twitter @acri_uts for updates, for news, and for our analysis.

Thank you very much. Bye for now.