Transcript: Q&A

Cyber-weapons are called viruses for a reason: statecraft, security and safety in the digital age

Professor Ciaran Martin

Visiting Professor, Department of War Studies and The Strand Group

King's College London

10th November 2020

Jon Davis: Good evening everybody. A very warm welcome to the forty-third Strand Group. I'm the director, Jon Davis. This is the very first King's event from our newest, illustrious visiting professor, Ciaran Martin, shared between the Department of War Studies and our very own Strand Group.

With a career spanning the Treasury, Cabinet Office and GCHQ, Professor Martin recently left government after founding the National Cyber Security Centre as its inaugural Chief Executive.

With a lecture entitled "Cyber weapons are called viruses for a reason: statecraft, security and safety in the digital age": Ciaran, you are most welcome.

[Ciaran's presentation to about 00:45:17]

Jon Davis: Thank you so much. I'm sure that everyone listening will certainly want to unpack that. If I may, I will ask the first question:

Listening to this, do you think the British government – with its multifarious components – do you think it's properly organised, as it is right now, for the threats and the opportunities that you have spoken about?

Ciaran Martin: I don't think the UK government is doing badly by international comparisons, and I was sort of gliding in and out of specific UK examples, but I think it's fairly common across the West, and the UK is in probably a better-organised position. I don't think the conversation is happening to as full an extent between the two communities in the UK, just like it isn't anywhere else; I don't think that you can have discussions about future digital conflict and so forth without the technologists, the industry people – frankly, citizen protection groups and so forth – for all the reasons I've set out. And I don't think governments are organised to deal with that.

That's understandable; these are hard problems. I don't think we've had a domain of potential conflict quite like this before, where it's just interacting so much, so often, with everyday activity. So I think, in the UK, there's much room for getting better at having this conversation; but I think, firstly, mindset-wise, it's a relatively short hop for the UK. I think some of the structures developed in the last ten years or so – the National Security Council and its subcommittees being an obvious one, where different parts of government come together; the fact the NCSC actually gives an open door to industry, and other campaign groups and so forth, and people who understand the technological aspects of this and its impact on civilian life, is another thing. So I think it probably starts with a head-start, [compared to] most Western countries – but it's not where I would want it to be.

Jon Davis: Thank you. OK, we'll turn to some of the questions here. First up is a former integral member of the Strand Group, Dr Ashley Sweetman, who asks:

What are the threshold criteria for deciding what constitutes a national security/digital public health threat? For example, is there a point at which an attack, say, on a bank becomes a national security threat rather than something to be dealt with by that organisation?

Ciaran Martin: As I suspect Dr Sweetman knows, that is a brilliant question, because in my view it's largely unanswerable. Every time I've tried to model things like this, reality proves you wrong, because there are at least three things here: there's the identity of the actor, which we know, in and of itself, can be a trigger that it needs to be taken as a national security incident; there's the identity of the victim, which could be so important that even if a criminal group that doesn't even know what it's attacking is attacking it, it's sufficiently important; and then there's the damage – so things like ransomware attacks on public authorities are of little strategic significance in terms of the identity of the attacker, but when it deprives British citizens of public services, then it's potentially a national security incident, depending on what that [service] is.

And I think, again, the UK's flexible governance and constitutional approach is quite helpful here; and the hybrid structure of the authorities we have – that straddle both national security and, if you like, civilian life – helps, because you can manage both. So I think we don't have a threshold; I think a lot of it is quite instinctive. I think when it is a hostile nation-state attack, that's most of the time an automatic trigger to get the security services interested, and involved, and think about those mechanisms of government; but it doesn't have to be, because the public impact can be so significant.

We didn't know for a long time, for sure, that WannaCry was a North Korean state attack, but we treated it as a major national incident immediately because it was disrupting the NHS. That's a way of thinking about it.

Jon Davis: Thank you. OK. I've got Zenia Douell, who asks:

How important is the cyber hygiene of the general public in cyber security?

Ciaran Martin: I think it's critical, and I think that it's what makes the open, free societies that we live in vulnerable to escalation, and that's crucial to the sort of theories that I'm setting out tonight. We are interacting through the digital domain, and I don't want to overstate or frighten people; I just think that the idea that you can have an escalatory cyber conflict that doesn't somehow then start to touch ordinary services, ordinary people's interaction – it's unlikely to hurt them, for a variety of reasons; there's always something else that has to be done to disconnect a power supply or whatever it is – but it can be a short hop from that sort of escalation to things that are genuinely and painfully disruptive of people's lives. And the incremental improvement in security of ordinary citizens and small organisations is one of the biggest things we can do to deter against that.

And that is why I think someone like Jason Healey at Columbia – in his work, in which he's probably more strident in these arguments than I am – would stress the gaping gap in the cyber defences of most Western countries, and the exposure that leaves them with in the event of cyber escalation. I think that might be slightly overdone, particularly in the UK, where I think it's getting better. So [in terms of] basic cyber hygiene, I think if you get to a position where the UK is considerably better protected in the digital domain at all levels – its critical infrastructure, businesses, and its ordinary citizens – then that is the platform by which you could perhaps reappraise some of the other

capabilities. I'm not sure that you *should*, but certainly I think that it is an absolute prerequisite for future digital prosperity.

Jon Davis: Thank you. Alasdair Ambroziak asks:

In the upcoming integrated review, there has been discussion about "sunset" capabilities such as tanks, and cyber investment mentioned as a "sunrise". However, it sounds like cyber needs to be seen as an additional environment rather than an alternative one. Do you think this is a challenge for policy makers, or is this well understood at all levels?

Ciaran Martin: I think it's a challenge, because it's very hard to combine the national security and strategic capability side of this with the fact that it's coexisting with consumer safety, which in my view it is. That is a really, really hard challenge. And I know that this is a very oversimplified "news story" type of reporting, but cyber capabilities versus tanks is not a sensible choice in my view. Thinking about the sort of digital society you want to be, and to what extent, I think you then have to work out the balance of defensive and offensive capabilities you want, for its own sake. And then you have to think about what place those digital capabilities have in your overall security strategy. So I think it's a very, very hard conversation to have, and that's why it needs to be broadened out.

Jon Davis: Our old friend, Gordon Corera, asks:

Would we be better protected from cyber attack if we were less dependent on foreign technology; or does more interdependence of technology around the world help deter the use of cyber weapons?

Ciaran Martin: It remains to be seen whether the growing polarisation of tech supplies will make us safer or less safe. It'll certainly be different. At the moment, I think that the integrated, very global, just-in-time supply chain – where even if something isn't from somewhere like China, it has a component and so on – has acted as a little bit of a deterrent; but at the same time, with technology, the way it works means that you can fix different bits of it that apply in your own country.

I think that if we move to a more, say, Western orbit of our own supply chains, providing we do it properly, with proper time, money and investment – and it will take time to decouple from the current very, very globalised supply chain – if we integrate security into that then I think, absolutely, there is an opportunity. But if we don't, that would be repeating the mistakes of the past: of the first generation of technology, from around the mid-1990s until the present, which has been designed without security in mind. It's one of the reasons why things like telecoms infrastructure need so much security improvement; if we repeat those mistakes, then it would probably actually leave us weaker than the status quo.

So it depends what we make of the emerging polarisation of the tech supply chain.

Jon Davis: Captain John Aitken of the Royal Navy says:

Thank you very much for an excellent talk: very, very interesting. Given the timescales involved in defence procurement (long), and the high cost of replacing high-end platforms, how can we best address retrofitting cyber security into those platforms – if we can do it, that is? We are operating platforms that were designed in the '80s in some cases; my fear is that the next Haddon-Cave inquiry will be looking into a cyber-security event.

Ciaran Martin: I'm not an expert on the cyber defence of military systems, and even if I was, there would be some things it would be wise and unwise to say in public. I would say that, whilst obviously legacy systems are a huge problem, one of the things that you see, for example, in the electoral

process is the fact that when you use very old-fashioned things, they can actually be less vulnerable. They may not be very efficient, and effective, such as the hand-counting (and hand-voting) of ballots in the electoral system, but at least they're impervious to cyber attack.

What we can do now to mitigate is two things: one is just patch and mend, and in the case of computer network security, I mean literally patch where patches are available. But the second thing is to model resilience and back-ups, and try and cauterise damage. That's been the most effective approach to legacy systems that I've seen: just to say, look, we realise that this is a weakness, but can you confine the damage if this is fully compromised? I still think the emerging catchphrase in cyber security, "Zero Trust" technology, applies very much to existing and legacy systems. This comes a little bit back to Gordon's point: with technology at the moment, as well as thinking about where it came from, just assume it's rubbish; assume that it's going to fail. And then work out what you would do. So that's some of the things that you can do, certainly in the military context, at the moment.

Jon Davis: Thank you. Dr Michelle Clement of the Strand Group asks:

Does the NCSC play a role in advising on NHS IT procurement with a view to taking preventative action re cyber attacks?

Ciaran Martin: Well I'm pleased to say that you'll have to ask the NCSC, and I don't claim to speak for it. I would observe, from my time and from recent annual reports and so on, that the answer is that certainly the NCSC works with the NHS very closely, and never more so than in the pandemic, when in my time – it's continued under my excellent successor – we steered up a huge protective operation. I think the defining moment was WannaCry, when we realised we needed to understand the NHS digital estate much better. Colleagues in NHS Digital have been extremely helpful in that regard.

In terms of big government procurement decisions that involve IT, like the NHS, I think it is still the case – certainly was when I left – that most big digital programmes have a cyber security advisory component. I say "component" because you don't want security people running the service, otherwise it'll be really secure; the only problem is you won't be able to use it. And when I ran the NCSC, we very much took that approach: that we needed to be a supportive function, and I certainly think you could see that supportive function in the NHS.

Jon Davis: We've got a question from the Treasury. Jon Fuller asks:

How do we square national security and economic prosperity?

Ciaran Martin: Well, you can invite another lecturer – not me, but somebody else – to talk about that! In terms of what I was saying tonight, I think there is a choice here. We are a digital nation – we are becoming a more digital nation – and that's incredibly important to our future prosperity; and I think there is an element of that which is to ask how we do the risk management for that, to a just about good enough state, so that we let digital innovation flourish, but do so in a way that doesn't compromise our security. There's then a question, frankly, of how much – in your projection of national security – how much do we want an assertive posture in cyber space to be part of that?

In my view – this is the crux of what I'm saying tonight – there is potentially a trade-off in that discussion: we want to be a very, very well defended cyber nation, but I'd just worry that some of this grey-zone, hybrid stuff, if we embrace it, is playing on adversary turf; and we don't need to do that, in my view… not often, anyway.

Jon Davis: Guy Faulconbridge, of Reuters, asks:

The head of GCHQ has spoken about the need to engage more with businesses to harness top cyber talent behind programmes to accelerate world-class technology. Have you any ideas on how that might work?

Ciaran Martin: I think there's a short-term and a long-term thing. The short-term thing is, whilst colleagues from the Treasury may not always, doctrinally, be in favour of it – there is a little bit of picking winners. Certainly, I think, one of the things the UK has done really well in the last few years is move public-private partnerships from conferences, and nice dinners – when we were allowed to have them – and committees, to saying, "Right, there's this problem, can anyone fix it because we'll pay you." The NCSC has got some good examples of that; other parts of government have got some good examples of that. And some of the things that GCHQ sponsor – like the accelerators for small businesses – are really, really good at developing that.

I think the long-term thing is about the education system: it's about STEM skills and so forth. I know often we've looked at the Israeli experience, which has of course been partly based on compulsory military service, and so to quote our old friend Sir Humphrey again, "That is a courageous policy, Minister." But there are things about incentivising, sponsoring people to do STEM; there's a huge thing about the female population losing interest at age 11-14, and whether we can do more about that, and earlier years education and so forth. So there's a short- and a long-term part of this.

Jon Davis: Thank you. Can Gökçen of the Strand Group asks:

In what ways are the demands of defending the cyber domain and environment changing twentieth-century concepts of security and defence, such as deterrence?

Ciaran Martin: So that's a brilliant question, and I'm not sure I'm going to give it a valid answer, because when I was writing this I was trying to think about to what extent is this a sort of digital version of the "war amongst the people" concept, and because I think this is very different to war, I didn't want to go there. I think at the heart of it is that for the first time in human history, an adversary – whether a criminal or a nation state – can do things systematically, at scale, without coming anywhere near your territory, or the territory of an ally. So when you think about that, it's not so much, then, that I worry about all-out war, and attacks and so forth, because in military history – and I'm not a military strategist – states and protagonists have sought to use the best technology available to them at the time of the conflict. That's pretty obvious. What I think is driving this change is that sort of large-scale harassment of the civilian population; of just the chronic socioeconomic harm that can be done; the attritional harm that can be done just through this constant wave of low- and medium-level attacks. That's where I think it's changed concepts of security.

Jon Davis: OK. We've got an anonymous attendee here:

Thank you so much, Ciaran; it was really interesting to hear from you with all your experience. Do you think our government needs to be more transparent, not just about its own capabilities, but also about those of our adversaries? It's obviously difficult to balance classified info with disclosable detail, but do you think more openness would act as a deterrent for the bad guys and as armour for the good?

Ciaran Martin: Yes. I mean there are limits; but yes – and I think it's all about your default position: you default to secrecy and you [allow] a little bit of openness; that's one thing. If you default to openness and then classify what you need to classify, that's where I would be. And I think the history

of technology shows that, by and large, when we've brought people with us, and explained choices and risks, we've done better than when we've kept things secret. And I think we should test everything we're doing, whether that's dealing with adversarial attacks or thinking about our own capabilities. I think we should always red-team it, about what happens if all this gets out: what is the justification for keeping all of this secret, given that some of it will be quite contentious? So I would default towards transparency, and I do worry that we're not doing that.

Jon Davis: Tim Stevens asks:

Thus far, we have seen limited escalation in cyber conflict. Is this due to the self-restraint of states, or is it a structural feature of cyberspace?

Ciaran Martin: Again, an excellent question. A little bit of both. It's both because they're linked. So the self-restraint is because, again, cyber is not a boxing ring: if you're not prepared to hit someone in the head with a physical weapon, most rational actors aren't prepared to hit them in the head with a cyber weapon either, because if you hit them on the head they're going to respond, whether it's [physical] or a cyber weapon. In terms of the incentive for restraint because of the way the internet is structured, I think the Thomas Rid stuff on this is quite interesting, and I would commend that "Cyber War Will Not Take Place" study that he did – it's aged very well for a seven-year-old book on technology.

I think that there is something around the fact that the advantages to cyber security aren't really in escalation. They're in gaining strategic advantage: in espionage, and that sort of thing. And I think even some of the rogue actors are very, very cautious, not least because at least two of the adversarial nations are proven to have done things that were utterly reckless – cost people a lot of money – and they probably don't want to be doing that routinely.

Jon Davis: Philip Dursey asks:

In the context of largely private infrastructure, what roles do you see for private governance, private law, and private intelligence/military companies in future cyber net-centric conflict, in terms of offensive cyber-operations, arbitration, etc?

Ciaran Martin: Right, so, two answers to that, that are very, very different. What role do I see for cyber-threat intelligence companies, antivirus companies and so on – [they're] great, and I know they have to deal with some very, very difficult things; I know sometimes that they have to weigh up very difficult ethical considerations and so on. But that part of the cyber security industry is a very, very important part of our civilian defences in pursuit of a safer internet. All the other stuff I'm *really* scared about – about corporate on corporate espionage, certainly in terms of private entities hacking back; I think the current law's in exactly the right place on that. And the gathering of legitimate cyber intelligence and so on for antivirus companies is fine, but private military companies and all of that sort of thing – having just spoken at some length about the militarisation and weaponisation of cyberspace, and the attendant risks, unsurprisingly I'm not hugely sprinting down that route.

Jon Davis: Emma Ling asks:

Hi. Thank you so much for your presentation; I found your HACKS framework very helpful. In my understanding, your focus on restraint contrasts with the American "Defend Forward" strategy. Is American cyber security on the wrong track, and if so, how can this be corrected?

Ciaran Martin: On the HACKS framework – I'm glad you like it – I actually think quite a lot of the Defend Forward stuff is what you might call very aggressive level two, and that's why – if you go back to it – the reason I drew a line between levels one and two and [levels] three, four and five is that you could argue that parts of level two, which is *directly* going after adversary infrastructure, are actually harder edged than level three, which is basically saying, go and poke around the energy network or we'll spread a bit of disinformation and all the rest of it. But I think a lot of Defend Forward is actually that really hard end of the second level: if you're going to attack the US or an ally, your infrastructure might well get destroyed. And that's [to do with] the Internet Research Agency, and there's all sorts of rumours, mostly in *The Washington Post*, about other activities that would all fit within that framework.

So I do worry that the West as a whole will start to go a little bit too far up the scale without really understanding what's at stake; but I think so far, whilst there are some really quite assertive aspects to Defend Forward, it's perhaps less far up the scale than one might think. I do however think – and one might expect an incoming administration to do more about this – that the domestic cyber-defences of the US are likely to be a significant priority for an incoming administration; I may be wrong, but I think they will be.

Jon Davis: Lilah Holywell asks:

I'm an online therapist. How significant is the online disinhibition effect on the evident need you've identified to urge caution?

Ciaran Martin: I don't know; I think the main reason why it can be hard to urge caution is actually just a slight misunderstanding of the way the technology works. It is a great question; I'm genuinely stumped. But if we're saying that people are just getting carried away, I'm actually not sure that is something, because decision-takers, who act, normally, in very restrained ways and very balanced ways, don't suddenly get very precipitous when they think about the online world. There is something – and other colleagues across the world have remarked upon this – about decision-takers – politicians, civilian officials and so on… and military decision-takers – just feeling that they don't understand it, but almost not saying so. And so then things get accepted with relatively little analysis: that there is a compelling case to do this, that and the other in cyberspace, without really weighing up and evaluating what's at stake. I think if you look at what the UK and other cyber-security authorities have done in the last few years with corporate Britain and corporate allied countries, it's quite interesting. We're telling people to just think about this as ordinary risk-management; just think about this as very ordinary activity. It's not a bad way of thinking about this, and then you don't get nonsense like "Where's the red button?"

Jon Davis: My apologies to those who've asked questions – we've run out of time, but I've got one last question here, from Ottawa, and our great friend James Lahey, who asks this very simple question:

What do you worry about most in this domain?

Ciaran Martin: Well, right up to my last day in government I worried most about a disruptive attack that would hugely damage a public service [using] criminal ransomware. I would always have been surprised if a nation state had just launched a big cyber attack at us without us seeing something coming; not because of technical aptitude – although hopefully that would have been an aspect of it – but there would have been some escalation of tension, or some observable escalation so that you were prepared for that. And then you would have been worried. But in the normal course of events, let's just take the recent experience of the US election. Our US colleagues did a superb job of

protecting us after what happened in 2016. But if you talk to the people, and look at their public statements, what they were most worried about – right up to the end – was that, given that elections are administered by small local authorities and state governments, a criminal would launch a ransomware attack – because they do it all the time on local government, in the UK and Europe and the US – and that it would just destroy their systems and stop their ability to administer the election, so that they could extort money out of them. Not that it would be Russia, or Iran, or anybody else. And that was always the worry I had: that we would have severe public disruption – to policing; to healthcare; to education; to child protection – because some criminal had ransomed a system. And I still really worry about that, because cyber is a peaceful domain of activity, and that's the most likely route to harm.

Jon Davis: OK. Well that brings us to an end. I think you've rattled through a huge amount of questions there; I think that this certainly deserves unpacking, in terms of the transcript but also the questions and answers, the recording of which will be up tomorrow.

And all that's left for me to say is that is a higher bar, Ciaran. Thank you so much – great respect, and we'll look forward to future Strand Groups with you. Thank you very much, and to everyone, for joining in and participating. See you next time.

Ciaran Martin: Thank you everyone.