



Defence Sub-Committee

Oral evidence: The Security of 5G, HC 201

Tuesday 2 June 2020

Ordered by the House of Commons to be published on 2 June 2020.

[Watch the meeting](#)

Members present: Mr Tobias Ellwood (Chair); Stuart Anderson; Sarah Atherton; Martin Docherty-Hughes; Richard Drax; Mr Mark Francois; Gavin Robinson; Mr Kevan Jones; John Spellar; Derek Twigg.

Foreign Affairs Committee Members present: Stewart Malcolm McDonald and Bob Seely.

Questions 48-108

Witnesses

I: Senator Tom Cotton, United States Senate.

II: Brigadier General (ret.) Robert Spalding, Senior Fellow, Hudson Institute; and Mike Rogers, Chairman, 5G Action Now.

Written evidence from witnesses:

– [Robert Spalding](#)



Examination of witness

Witness: Senator Tom Cotton.

Q48 Chair: Welcome to this Defence Committee hearing to consider the international response to the UK Government's decision to allow Huawei to continue to operate its 5G network, and the implications of that decision for information sharing across the alliance. We will also discuss international ambitions and the role of 5G technology. Within that, we will specifically look at cyber-attacks and the digital silk road.

Our session today is divided into two parts. I am delighted to welcome Senator Tom Cotton, who is joining us for part 1, and then Brigadier General Robert Spalding and Mike Rogers will join us for part 2.

Senator, thank you very much indeed for your time today. You are ex-military, and you sat in the House of Representatives before being elected Senator. You are a regular commentator on US foreign affairs, and particularly on the US and China relationship. For transparency, you and I have known each other for many years—prior to you entering politics. Thank you very much indeed for your time today.

On a wider note, we are very conscious that we meet during a challenging time for the US, following the tragic death of George Floyd. Our thoughts are very much with those impacted by this tragedy. The US is not alone in needing to do more to tackle the underlying issues. Our thoughts and prayers are very much with those who are directly affected. I invite you to say a few words as an opening statement, and then we will move into our questions.

Senator Tom Cotton: Thank you, Chair, for those kind words about the strife that we see on our streets today. Of course, we all want justice for George Floyd, and we are all deeply disturbed by the horrific video that probably all of you and the citizens of both our nations have seen. We respect the right of peaceful protesters, but at the same time we have to have an end to the violence, looting and rioting that we see on our streets.

Today, we are gathered here to talk about China, and specifically the threat that Huawei poses to our special relationship and the civilised world. I have a few remarks at the outset on that front. I want to make it clear that I am not here on behalf of the United States Government. The views that I express are solely my own, although I believe that they are widely shared in our nation's capital.

I also want to stress that I am a great admirer of the United Kingdom and a passionate supporter of our special relationship. In recent years, I have introduced legislation that halted a planned withdrawal of forces from RAF Mildenhall, and I have also helped to fight budget cuts that would have significantly delayed our joint development of a warhead for your new submarines. Both those efforts were successful. It is my hope that the special relationship remains strong, although I fear that China is attempting to drive a high-tech wedge between us, using Huawei.



HOUSE OF COMMONS

The Committee has access to testimony from very capable specialists about why Huawei equipment is untrustworthy. I understand that your Government has been advised that the threat from Huawei can be contained if it is kept away from sensitive facilities in the so-called core of your network. I will not wade too deeply into that technical debate, but I will note that our own technical experts disagree, as do the experts in allied democracies like Australia and Japan. These same experts also warn that Huawei could help China obtain a host of damaging information, from details about how our aircrews fight to intrusive personal information about our airmen themselves. They warn of scenarios where the Chinese Communist party could acquire compromising details about American forces stationed in your country.

Let me give you just one hypothetical—one of many I could offer. Our fighters in England are armed with precision-guided munitions by ground crews using special lanyards shipped from the United States. Those lanyards are transported by shipping companies operating on standard commercial networks. If that network includes Huawei 5G equipment, it could give PLA hackers a window into our military logistics operations, including shipping manifests for those lanyards. Hackers could then redirect or cancel the shipments, making it impossible to load these weapons and putting fighter crews in our missions at dangerous risk. These are the warnings of American experts, and as an elected official here, I must take those warnings seriously, even if our friends in the United Kingdom have come to a slightly different conclusion.

There is also another consideration that I must bring to your attention. Today, we judge the threat in the Western Pacific to be more severe than the threat in Europe. China is a graver long-term threat to international peace and stability than Russia is, so, in the coming years, the United States plans to increase our defence posture in the Pacific. That build-up may require us to ship assets from other commands. The case for a heavy lay-down of air force assets in England rather than, say, Alaska, Hawaii, Guam or Japan was already contested in our debates in Washington. Now, senior US officials are realising our troops will face an operational security risk in the United Kingdom, that they would not otherwise face in the Pacific.

I say all of this as a long-time defender and friend of our special relationship. It would be a mistake for any British lawmaker to misinterpret this potential realignment of US forces as a bluff or a simple messaging effort. We believe our airmen could be at risk. We have a greater threat in a different hemisphere and will have a limited number of forces to deal with it. These are simply facts that are under consideration in Washington right now.

However, there is another path. Britain can join the United States and other powerful free nations and work together on a 5G solution that does not empower Chinese intelligence. I am greatly encouraged by reports indicating that your Government intend to help lead efforts to develop alternatives to Huawei among the world's democracies. I would welcome



HOUSE OF COMMONS

even closer co-operation between our nations on these matters. It is no secret which of these futures I prefer, but the decision, of course, is yours to make.

Thank you again for inviting me to share my perspective as you make this important decision.

Q49 **Chair:** Senator, thank you for those words. There is lots to unpick there, which the Committee will now do.

I want to start at a higher level, if I may. You mentioned the special relationship a couple of times. Would you agree that the pandemic that we are now enduring has exposed in sharp relief how frail our world order currently is and perhaps how weak and risk-averse the West has become, as well as the rise of China in pursuing a very different geo-political agenda—and that many may be recalibrating their views on China, given what they have been doing in relation to Hong Kong and in covering up and suppressing the outbreak in the first place? How might that lead us to the United States and Britain going back perhaps to the origins of our collaboration after the second world war and looking at the Atlantic charter?

Senator Tom Cotton: Mr Chairman, there is no doubt that the scales have fallen from a lot of eyes when it comes to Chinese Communist behaviour over the last six months. Going back to December, it is clear that Beijing had knowledge of how serious this virus was. They suppressed that information. They intimidated the World Health Organisation from releasing it. As late as mid-January, they continued to resist the kind of travel restrictions that would have kept the virus largely contained inside mainland China. They continue to do those things—intimidating the European Union from offering an honest opinion about Chinese disinformation efforts and, just in the last week, the Chinese have obviously cracked down on Hong Kong, in deep violation of the commitments that they made to your nation in 1984.

In the United States, we see public opinion moving strongly against Beijing, desiring to have closer co-operation with free nations, with the civilised world, on things like industrial sourcing, to ensure that China cannot keep any of our nations under a barrel, whether with things like basic medical equipment and pharmaceuticals, or advanced telecommunications technology, as we are discussing today. That situation, as you say, simply reiterates how important it is for our nations to co-operate and to help lead that coalition of advanced industrial democracies.

Combined, economically, politically and militarily, we are far greater than China in terms of strength, power and ability to maintain international stability and peace. Divided, though, and China will continue to try to replace the United States as the dominant power and to rewrite the international rules of order.

Q50 **Richard Drax:** Good afternoon, and nice to meet you—as far as one can virtually. We have heard about the special relationship. Is there greater



scope for US-UK leadership in the modern world?

Senator Tom Cotton: Thank you, Mr Drax. I think that there is no doubt about that. That is part of what Brexit was about—the United Kingdom being able to chart its own course and not have to reach a consensus with a couple of dozen other different nations. With that greater freedom of action, which the United States continues to enjoy, there is no doubt that US-UK leadership once again would be welcomed. Many nations could use our combined political, economic and military might. Look, for instance, at what Australia, one of our Five Eyes partners, is facing in trade retaliation by China, simply because the Australians wanted an investigation into the origins of this virus and into what Beijing did to cover it up. A strong, confident and united US-UK alliance will in fact be a strong leader for the free democracies of the world.

Q51 **Richard Drax:** Is there anything specific that the two countries should do, in so far as leadership is concerned, today?

Senator Tom Cotton: To go back to the topic of this hearing, 5G technology, one of the challenges we will face is that 5G technology is still nascent. We do not know where it might be in three years or, for that matter, even in six months, because the technology changes so quickly.

Part of the problem we will face is that there are so few providers of 5G equipment: two are supported by and are essentially arms of the Chinese Communist party; and only three are democratic alternatives, Samsung, Ericsson and Nokia. That has in part allowed them to keep technology and standards locked down.

If the United States and the United Kingdom were to lead the way to develop open standards, as your Government suggested last week, small and mid-sized businesses in the thousands in our nation, your nation and nations around the world could compete with those five companies on price and quality. No longer would Huawei and ZTE, because they are so heavily subsidised, be able to undercut those democratic alternatives on price.

That is just one example of how we could lead the world with this kind of cutting-edge technology and ensure that the international order remains oriented on democracy and capitalist economic principles.

Chair: On that issue of the international order and perhaps its strengths and weaknesses, Stuart Anderson, will you take over from here?

Q52 **Stuart Anderson:** Thank you, Chair, and hello, Senator. We have talked about decisions that we as countries could make in different relationships. At the moment, would you say that we are seeing a paralysis of our current international decision-making architecture?

Senator Tom Cotton: I think there is some indication, yes, that international organisations in particular are struggling to meet the challenge that China poses. That is in part because China has worked so effectively to try to undermine, and to insinuate itself into, the central decision-making places in those organisations. You can look at the World



HOUSE OF COMMONS

Health Organisation, for instance, and Chinese cultivation of senior leaders there, done to the extent that our President has decided that the United States can no longer have the confidence to remain a member or fund it. Or just look what happened two or three months ago, right as this pandemic started: China was on the verge of electing a leader of the World Intellectual Property Organisation, of all things, when China is in fact the world's leader in theft of intellectual property.

Now, thanks to an effort by our Government and yours and other free nations, we were able to run an effective campaign to beat the Chinese-backed candidate, but it goes to show you how concerted an effort China has undertaken in some of these international organisations. Even if you look at the EU, you have divisions there among nations that have been actively cultivated by China, whether through low-interest loans and grants, things like the belt and road initiative, or trade concessions and so forth. I do not think there is much question that China has had some influence in reducing effective and united decision-making among the free nations of the world, and especially of the north Atlantic. That is something that our nations need to address.

Q53 **Stuart Anderson:** Thank you, Senator. We could say that we are on the back foot on a lot of these, or being very reactive. How would we amend organisations such as the UN or the World Trade Organisation to be more fit for purpose, based on what you have just said?

Senator Tom Cotton: We have to recognise that China is not a country led on democratic capitalist principles like ours. In fact, admitting China to the World Trade Organisation was a mistake, or you might call it an experiment that failed—one that failed a long time ago, and should have been ended a long time ago.

Our nation made a mistake by granting China permanent most favoured nation status. We all believed that if we did those things—by “we”, I do not mean any of us in particular; I mean our forerunners in these offices, in Washington and in London—if we admitted China to those organisations and treated it like an open, capitalist, democratic economy, that China would be become more so: that capitalism would change China.

Unfortunately, I think China has changed capitalism in many places around the world, so we need to reassess whether continuing to allow these international organisations to give such a large role in decision making to what remains a communist, authoritarian Government and a state-driven economy is the right thing to do. Until we face up to that reality and make those kinds of decisions, China can continue to throw sand in the gears of the institutions that our two nations set up in the aftermath of World War Two, whether political, diplomatic, economic or military.

Q54 **Stewart Malcolm McDonald:** Senator, thank you for giving us your time today. Just like the Chair, I would like to echo the sentiments of many in the UK who believe that black American citizens right now really deserve better.

Senator, you mentioned that you are a supporter and admirer of the



HOUSE OF COMMONS

special relationship. Quite rightly, there has been no shortage of frankness on the US side as far as the Huawei 5G decision goes; I am in agreement with you about the UK decision. However, on the issue of American leadership and the special relationship, some of us—myself included—feel that it is currently being undermined, especially by the US presidential leadership, and particularly as it withdraws from organisations such as the World Health Organisation and treaties such as the open skies treaty. Does the US retreating in this way not just leave greater opportunity and attack surface right across the board for authoritarian regimes?

Senator Tom Cotton: No, I have to disagree with that. If anything, I think it gives opportunity for the free democracies, especially those of the northern Atlantic, to try to help remake world order and maintain peace and stability, just as our forebears did in the aftermath of World War Two. We understand that we will have disagreements, whether they come from the open skies treaty or the Paris climate accord, but our relationship will work through those disagreements.

Q55 **Stewart Malcolm McDonald:** How is the world safer with the US out of the WHO, though?

Senator Tom Cotton: We can help refound a new organisation that is a world health organisation, not a world politics organisation, as the WHO has become. You had your disagreements about Brexit, as well—obviously, very intense disagreements that caused a lot of division in your society for many years. We watched that with great interest. We in our society had people who supported the leave campaign; we had people that supported the remain campaign. Whichever one had won—whichever path you had chosen to take, though—we would have respected that decision and we would have remained your staunchest ally. That is what it means to have that special relationship—to have those kinds of allies: that when it comes to disagreements we face them frankly but we do not let them undercut our fundamental, long-standing deep ties, that go back to the very way we live our lives.

Q56 **Stewart Malcolm McDonald:** Don't you think it is a bit risky to withdraw from the WHO in the middle of a global pandemic? That strikes me as a bit odd.

Senator Tom Cotton: Not when the WHO has taken so many steps that actually made that pandemic worse, by kowtowing to Beijing in December and January. The President gave them an opportunity to try to reform, and try to be more open and transparent. They did not take that opportunity for 30 days.

Q57 **Stewart Malcolm McDonald:** Apologies for interrupting, Senator, but this is kind of my point. This is not standing up for our values—and the 5G debate is as much about values as it is about security. It is retreating, it is running away, and it leaves a greater opportunity for authoritarian countries around the world. I, too, admire the United States. It has played an honourable role in many events in history. It has produced some incredible thinkers; but I cannot help but think the current



HOUSE OF COMMONS

presidential leadership, and in particular his style of leadership, is grossly undermining that—and that is certainly felt by not just many of my constituents but people from all political persuasions in the UK right across the board. So I hope you can see that. I hope you can understand that point, as a law-maker in the US.

Senator Tom Cotton: I do see it, just as I saw it for Ronald Reagan and George Bush, as well.

Chair: Okay, we will move forward, if we can. Sarah Atherton, do you want to take us on to look at the Five Eyes aspects of this?

Q58 **Sarah Atherton:** Hello, Senator. You touched on Five Eyes earlier, but how valuable is this intelligence alliance?

Senator Tom Cotton: Five Eyes is the most valuable and the most powerful intelligence alliance in the world. For 75 years it has helped us identify threats and in many cases eliminate those threats in advance of them gathering on the horizon. I do of course worry that the introduction of Huawei technology in the United Kingdom's 5G network could impact our ability to share the most sensitive intelligence. Of course we could find ways to work around that—especially when it relates to imminent threats; but when it comes, in particular, to signals intelligence, electronic intelligence, I worry—I know our Administration worries—about the implications of having 5G technology in one of those five partners. Of course, three of the partners have rejected 5G technology from Huawei, or China at large—the United States, Australia and New Zealand. Canada has not yet made the decision. I know their chief of defence, though, has made his opinion plain—that he agrees with our nation. That is one reason why I hope that we can present a united front among the Five Eyes partners on this question.

Q59 **Sarah Atherton:** How much of a threat will be the breaking down of relationships, perhaps? You mentioned signal technology but, taking that to one side, you mentioned three countries are going in one direction; Canada has not decided. How much of a threat to Five Eyes would it be if the Government continues with its plans for Huawei?

Senator Tom Cotton: It will create some tensions in our ability to share the most sensitive kinds of intelligence. Legislation passed last year calls for our intelligence agencies to consider the extent to which partner nations have Chinese-sourced technology in their networks. I have introduced legislation that would take a step further. The NSC, our National Security Council, is undertaking its own review. Now, again, we would find a way to work around on the most urgent questions of sharing intelligence—sharing analysis or sharing the kind of imminent threats that of course we always pass between our five nations; but there is no doubt that our intelligence agencies would face some challenges in being as open and sharing as much information—particularly information, again, in the signals intelligence arena—that they do now and that we have for so many years, and I would hate to see that come to pass.

Q60 **Chair:** Thank you. Just before we turn in more detail to telecoms security,



HOUSE OF COMMONS

can I just go back to the Five Eyes? I think we all agree that China is pursuing its own global rules; it is not playing by the standards and values the rest of us were hoping it would adopt. Indeed, it is leveraging the absence of our ability to enforce those rules. Could the Five Eyes community be the core of something that allows us to rebuild international standards and values? At the moment, it is known for sharing intelligence, but is the trust that you have there perhaps the genesis of advancing an Atlantic charter thought and setting out a new construct or set of values and norms that we can absolutely defend?

Senator Tom Cotton: I don't think there is any doubt that Five Eyes intelligence-sharing nations have many deep economic, political, historical and cultural ties that could be a foundation of more than mere intelligence-sharing. Our nations are already so close together in so many ways that we could form the core—along with many other friendly nations, especially nations whose co-operation will be essential in this effort, such as Japan and South Korea—to help establish some of these new standards, whether they are technological standards or international political standards.

Chair: Thank you. Kevan Jones, do you have a quick question before we move on to telecoms security, please?

Q61 **Mr Jones:** Just on Five Eyes, Senator, I don't think you have read GCHQ's documentation around Huawei, but I also sit on the Intelligence and Security Committee, and there is no evidence at all that anything about co-operation between our two nations is going to be compromised by what is being proposed. So, is this not just being used as a threat to try and change policy, a little bit like your proposal to stop deployment of F-35s to the UK, for example? You talk about the special relationship and say you value it, but you said earlier that it would be down to the UK to make its own decisions. Aren't these things really just being seen as threats to try and change policy in the UK?

Senator Tom Cotton: No, I have to say not. I think that is letting the wish be father of the thought. I mean, the simple fact is that our National Security Council is undertaking this review right now, because—

Q62 **Mr Jones:** But there is no evidence. It is very clear from GCHQ and our security agencies that there is no way that Huawei equipment will come anywhere near anything in terms of our signals intelligence, or impact on yours.

Senator Tom Cotton: This gets into the debate about the so-called core and the edge, which is, again, a technical debate. Our experts, just like Australia's and Japan's, disagree. I would ask this: why are you so eager to put a criminal organisation's technology into your networks?

Mr Jones: Senator—

Senator Tom Cotton: I am speaking now; please let me finish. This is an organisation whose technology is being used to repress millions of minority Muslims in Xinjiang province, and which is a serial sanctions



HOUSE OF COMMONS

violator, building up the networks in Iran and Syria. You seem very eager to use their technology. Why would you be so eager to use their technology?

- Q63 **Mr Jones:** Senator, to use an Australian phrase, I am no panda hugger; I have been a member of the Taiwanese all-party group since I was elected 19 years ago. What I want to do is actually deal with the facts. The point is that GCHQ have looked at the issue, and the Government have looked at the issue. In terms of Huawei equipment, you have it in your networks, and we have it in ours. What has changed?

Senator Tom Cotton: As I said, our experts have looked at it, and they disagree. I am not an expert, but—

- Q64 **Mr Jones:** But Senator, you have Huawei equipment in your 3G and 4G local wi-fi networks in the United States. Are you going to rip all that out?

Senator Tom Cotton: Yes, we are. In fact, we are providing money to some of these very small, very rural telecom providers so they can remove that technology. And to compare British use of Huawei technology, which I believe is well over 50%, to American use, which is a trivial fraction of a percent, is to miss the point.

Mr Jones: Well, it's not.

Chair: Okay. We need to move on. Kevan, thank you for that. Martin Docherty-Hughes.

- Q65 **Martin Docherty-Hughes:** Thank you, Chair. First of all, let me associate myself with the comments you made, and especially the comment of my colleague and friend, Stewart Malcolm McDonald earlier today. While we will agree and also disagree today, Senator—I think you might be quite shocked at some of the agreements I will have with you, but I will disagree with some of the comments you made last night on Fox News regarding the deployment of the 101st Airborne—what I will agree with you on is that handing over your 5G network to the Communist party of any country is utter insanity. What I would like to ask you, though, is, with a world relying ever more strongly on data, why is the security of telecoms networks so important?

Senator Tom Cotton: Thank you for the question, because it is sometimes misperceived that the 5G networks that are currently being designed, and that will ultimately be built across the world, are somehow just an incremental step forward from 3G and 4G technology. That misapprehends the leap we are taking. In some ways, the information technology revolution through which we are living now is as big as the industrial revolutions 200 years ago or the agricultural revolution 10,000 years ago. The 3G technology was primarily about mobile web browsing, and 4G technology was primarily about video, but 5G technology is fundamentally about connecting machines. It is not about being able to access social media faster or sending more selfie videos over your devices; it is about pieces of heavy industrial equipment being able to communicate with each other, and autonomous vehicles on the road being able to



communicate directly with each other. That is such a giant step forward in technology that a difference in degree really becomes a difference in kind.

When you are talking about a 5G network that is primarily about ways we can connect machines to do the economic work we need to support our societies, but also about the military implications that come with that, it becomes a much graver threat to have Chinese technology in 5G networks than it was to have it in 4G and 3G networks. I should be clear that I am not thrilled that so many countries have built 3G and 4G networks in the past, because it creates some of these transition costs that your nation or other nations are going through. But the risk is much greater with 5G networks, and that is one reason why it is so important that we try to collaborate to create open standards that eliminate the locked technologies that we face now that create so many problems. We have only five competitors, and only three competitors from democratic nations.

- Q66 **Martin Docherty-Hughes:** Let me ask a quick follow-up to that. The 5G process is one part of data ownership. Future conflicts are not just about dreadful missiles and the destruction of human life. This is also about Governments and non-state actors owning data—and not just the Communist party of China. For example, if you take the United States, Amazon has the largest private super-server data network in the world. Where would your allies, and even those who threaten you—your enemies or perceived enemies—see the value and worth of the United States owning all our data via their own private companies?

Senator Tom Cotton: The United States will not own all that data. Some companies in the United States may have substantial amounts of data. Most of it has been given over voluntarily, but that raises a lot of personal privacy concerns. Those concerns are similar to what I raised in my opening remarks about what our airmen could be exposed to in nations that are using 5G networks. That is a conversation that our elected Governments need to have, about how we balance personal privacy on the one hand and individual economic choices on the other hand.

- Q67 **Martin Docherty-Hughes:** Forgive me for pushing this slightly once more, Chair, but it is important for those of us who believe in liberty, freedom and the right to self-determination, such as myself. The ownership of that data is the frontline in any future war, in terms of articulating fake news and racial profiling in any country on earth. It is a concern if any country is not taking that seriously, especially when that data ownership is by private companies in the largest democracy in the world.

Senator Tom Cotton: I understand those concerns, and, trust me, those are concerns that many, many Americans have as well. It is one of the reasons why you see so much on the news now about the telecom laws that govern some of our largest media technology companies.

Chair: We need to make progress here, because we still have a lot to cover. Kevan Jones, we will quickly move on to your question, please.

- Q68 **Mr Jones:** The United Kingdom has, since 2003, always had robust



HOUSE OF COMMONS

monitoring of Huawei in its telecoms network, with the Huawei assessment centre that is overseen by our intelligence at GCHQ. Will you tell us about America's own system for defending its own network?

Senator Tom Cotton: Obviously we have similarly robust protections, whether it's from our FBI, in the work they do in counter-intelligence with the National Security Agency, or in terms of the simplest way to minimise the Huawei threat, which is not to have Huawei present in your networks to begin with.

As I mentioned in our earlier exchanges, we have a very small Huawei presence, limited primarily to a few small rural telecoms, which go back many years, to before the threat that Huawei and ZTE pose was recognised. Our Government recognise that now, which is one reason why we are providing finance for those small companies, to help replace their technology and their networks.

Q69 **Mr Jones:** I understand that some of those networks were put in using federal money. Will Huawei have no presence in the United States at all? For example, will you be banning handsets provided by Huawei in the future?

Senator Tom Cotton: I would be fine banning handsets. They don't pose the same kind of threats that core technologies do. They also have virtually no market penetration in the United States.

Q70 **Mr Jones:** Senator, I respect your position and, frankly, I am an Atlanticist—I value our special relationship. The problem is that if this is a geopolitical argument, which I accept it is, that is what it should be articulated as. I think you, and quite a lot of other people, skirt around the technical aspects of this. If you want to say that you don't want China in the network, that's fine by me. That is a legitimate argument, but some of your arguments don't stand up to a great deal of scrutiny when it comes to technology.

Senator Tom Cotton: I'm not hiding behind any argument here. A division of your own National Cyber Security Centre have said they can only give limited assurances about the threat that this poses. The US Government, the Australian Government and the Japanese Government—

Mr Jones: No, read the report, Senator.

Chair: Kevan, we are going to have to move on, because many other Committee members want to get in. Bob Seely, the floor is yours.

Q71 **Bob Seely:** Thank you, Mr Chairman. Senator Cotton, I am glad you were about to make that point, because I was about to quote it as well. Our own National Cyber Security Centre says that there are going to be very limited assurances.

Moving on to my question, you introduced a Bill that would stop the US from sharing intelligence with countries that use Huawei in their 5G networks. Do you think the Five Eyes can survive if the US limit intelligence sharing with the UK?



HOUSE OF COMMONS

Senator Tom Cotton: I do. As we discussed in my exchange with Sarah Atherton earlier, we will find ways to continue to co-operate with the United Kingdom and the rest of the Five Eyes alliance. Unfortunately, it could raise challenges. Our own National Security Council, irrespective of the prospects of my legislation, is undergoing a similar review on its own accord. I hope the result of that review is that we can find ways to minimise that risk, with very limited change to the way the US and the UK interact in intelligence sharing, and the Five Eyes intelligence sharing, but part of my point here is that I wish we didn't have to undertake that review. I wish we didn't have to face that kind of risk and mitigate it.

Q72 **Bob Seely:** What kind of challenges are we talking about? Is it just practical ones? You used the example of US servicemen and women being based here. What sort of range of challenges are we talking about?

Senator Tom Cotton: Again, a lot of it goes back to signals intelligence and the sensitivity of sources and methods. Some of these things we can't discuss in an open setting, but they are concerns that our intelligence professionals and our technical experts have raised about not just the United Kingdom using Huawei, but any nation that uses Huawei technology.

I want to correct something that one of the Members said earlier about my legislation—that it would delay the deployment of F-35 fighters to the United Kingdom. It does not delay them specifically to the United Kingdom. It simply says that it raises too great a risk for us to have that advanced aircraft in any nation with this system. Obviously, the United Kingdom is not the only nation that uses Huawei. We will have to face that threat in other nations that choose to use Huawei to build up their 5G network.

Q73 **Bob Seely:** Is this just a question of geopolitics, as was raised in a previous question? What is the extent of the balance between geopolitics and technical risk for you? Is it all wrapped up in the same issue around China?

Senator Tom Cotton: It is all wrapped up. The point I was discussing earlier is that 5G technology is such a technological leap beyond 3G and 4G technology. It is so central to the way economies will function in the future and the way our countries will secure themselves that I believe using Huawei technology, using ZTE technology or using any technology from a company that is beholden to the Chinese Communist party would be as if we had relied on adversarial nations in the cold war to build our submarines or our tanks—it is just not something that we would have ever considered. There are certain technologies that are so sensitive and so integral and vital to our prosperity and security; we would never use an adversarial nation for such technology. That is an analogy that I see today with 5G technology.

Chair: Can we turn to the US National Security Council? Derek Twigg.

Derek Twigg: Hello, Senator. Can I draw you out a bit more in terms of—
[Inaudible.]



HOUSE OF COMMONS

Senator Tom Cotton: I'm sorry, Mr Twigg. I am having trouble hearing you.

Chair: We all are. Derek, can you speak up a bit?

Derek Twigg: Can you hear me now? Can I draw you out a bit more in terms of the—*[Inaudible]*—led by the National Security Council in the—*[Inaudible.]* If the UK Government continues to stick to—*[Inaudible]*—what do you expect will be the outcome of that review?

Chair: I could hear some of that, Senator. Do you want me to feed that back to you?

Senator Tom Cotton: Please.

Q74 **Chair:** There is a review that the US National Security Council is looking at, into sharing intelligence in collaboration with the UK. Can you spell out what outcomes have been provided from this?

Senator Tom Cotton: Unfortunately, Mr Twigg and Mr Chairman, I cannot spell that out, because I cannot speak for the National Security Council and, ultimately, for the President. As I stressed at the outset, I am expressing my views today as a legislator. I can say that that review is not specifically about the United Kingdom; it is about the broader question of intelligence sharing with any partner nation that is using Chinese technology in its networks. Whatever the conclusion of that review is, I know that our Administration will work to find as many ways to mitigate the risk as they can—in particular, to mitigate that risk with the United Kingdom, which is our closest intelligence partner in the world.

Q75 **Chair:** Derek, if I may, because of your sound, I will follow on with the subsequent question. We spoke about the demise of international institutions and global architecture. NATO is the cornerstone, from our perspective, to our security—European and transatlantic security. Are you committed to making sure that this is one cornerstone that continues to be of strength and invested in?

Senator Tom Cotton: Yes, absolutely. NATO will remain a vital part of the United States' national security strategy. The North Atlantic Alliance has been the most successful military alliance in world history, if you look at what we accomplished by bringing an end to the cold war without a shot being fired. Many of our leaders have awoken to the risk that, unfortunately, Russia still poses to the north Atlantic over the last five or six years, and to the fact that, more than ever, the United States and Canada need the support and co-operation of our European NATO partners to help check Russian ambitions in Europe.

Q76 **Chair:** Following on from that, we are all facing an impending global recession because of covid-19. One of the budgets that often gets challenged in times of economic downturn is the defence budget. You would not be surprised to hear that this Committee is very keen to make sure our budget is unaffected. I don't know what will happen over in the United States, but do you agree that this is not the time to let our guard



down?

Senator Tom Cotton: Absolutely, I agree that we need to ensure that our militaries are not harmed by this pandemic—especially in the years ahead, as we face budgetary constraints. I have introduced legislation that would help offset many of the cost and schedule overruns that our defence industries will obviously face. Here, as I'm sure there, there is a lot of media attention on businesses that are consumer-facing. There is not as much attention on our defence industry, but they, too, have been affected by this pandemic—in particular, small and mid-sized businesses that are military suppliers have had to shut down factories or go to reduced hours. Inevitably, through no fault of those contractors, that will lead to some cost overruns and schedule overruns. I do not want to see that lead to lower budgets in the future or, even worse, a reduction in the number of aircraft, ships or vehicles that we are able to produce. I would also say that, collectively, NATO or the free world has probably upped its spending now by around \$6 trillion or \$7 trillion on trying to survive this pandemic and get our economies back on their feet. When we are spending that kind of money, to not spend a few billion or tens of billions of dollars collectively, between all our nations, would be the ultimate example of swallowing camels while choking on gnats.

Chair: We will pass that on to our Chancellor. Thank you.

Q77 **John Spellar:** Senator, I think you can see from this discussion how this issue has caused divisions between traditional allies, not least between myself and my old party friend and defence colleague, Kevan Jones—we are normally allied on issues.

I want to move now to the question of what China's intentions and actions are more broadly, and particularly their increasing combativeness—the "Wolf Warrior" diplomats and other manifestations—and also to ask how you see their strategy and objectives playing out over the next 10 to 15 years.

Senator Tom Cotton: Thank you for the question, Mr Spellar. To me, China's ambitions are pretty straightforward. You can see them in their actions, but you can also simply listen to the words of Chairman Xi. In the short term, they want to try to push the United States and our allies out of the littoral in the western Pacific and the Indian ocean. They want to reduce countries on their periphery to vassal states, as they have been so often over the course of history. And they want to reunify what they perceive to be all of China, forcibly, if necessary, with Taiwan. I think you can see that Hong Kong is something of a test run for what they might plan to do with Taiwan if the free world does not stand steadfast with that democratic people. So I do not think their intentions are concealed or veiled in any way.

Ultimately, their long-term intention, up to the 100-year anniversary of the founding of modern Communist China—they may have accelerated that thinking, because of the impact of the pandemic—is to replace the United States as the world's pre-eminent economic and military power,



with all that that means for reordering the international rules of peace and stability.

- Q78 **John Spellar:** Isn't one of the advantages they have that they are maybe being a bit more strategic than we and our allies are? For example, with Huawei, have they not had a strategic objective of sowing dissension and division among allies? Should we not be looking far more at a strategic, coherent and agreed approach?

Senator Tom Cotton: Well, it is true that China has had a remarkably fast rise of the last 30 to 40 years. Unfortunately, too many people in the United States and Europe have aided and abetted that rise, even once it became clear, in the last 15 or 20 years, that China's intentions were not benign.

I think it is also true that democratic peoples can often look at authoritarian Governments and say, "They have advantages because they have one strong man. They can direct capital to state uses like Huawei and ZTE." But history has shown us time and time again that the advantages of democratic nations, in terms of the dynamism of our people, their innovative spirit and the willingness to stand and fight for our freedom and our way of life, are an incalculable advantage that we have over communist, authoritarian nations.

Of course, we have divisions. As your greatest statesman, Churchill, said, "There is only one thing worse than fighting with allies and that is fighting without them." I guess you could say that about some peaceful decisions, as well. But in the end, I am confident that if we stand together, despite our occasional differences, and recognise China's malign intentions, we will be able to face off against this threat, just like we have time and again over the centuries.

- Q79 **Mr Francois:** Senator, you mentioned earlier on that there are a very limited number of providers around the world that can manufacture high-end 5G technology. When this Committee has taken evidence on this matter before, one of the things we have focused on is why there is no American manufacturer as such. Why do you see that being the case?

Senator Tom Cotton: Sadly, I think it's the result of failed economic and trade policies going back 30 years, that we could outsource so much of our manufacturing capacity in so many different sectors of our economy around the world to include a hostile communist nation like China. We have just lived through the peak of a pandemic in which we were worried about having enough masks and gloves for our doctors and nurses. We are still worried about China having the market cornered, to a degree, in vital pharmaceuticals. There has been a degree of economic thinking over the last 20 to 30 years that prioritised market efficiency over every other economic principle. That is a very important principle—don't get me wrong—but resiliency in production is a very important one as well.

I wish we had an American producer on the scale of Samsung, Nokia or Ericsson. We do have a lot of small and mid-sized companies that could possibly compete with those giant companies, if they had the kind of open



HOUSE OF COMMONS

standards and technology wasn't locked up. I am sure that AT&T and Verizon and a lot of our small providers would love to be able to choose between dozens of manufacturers of this equipment, as opposed to just five worldwide and only three democratic ones. There really needs to be a vitally urgent effort on our part, on your nation's part and on the part of advanced democracies everywhere.

- Q80 **Mr Francois:** Part of the heart of 5G will be software as much as hardware. The United States has companies like Cisco that are very far advanced in those fields. Senator, would you agree that between us we have the technology and the nous to create a western 5G system, if we have the will. Do you think that is something the United States and the United Kingdom, historically as allies, could help to lead on in creating, if you like, Five Eyes 5G?

Senator Tom Cotton: Yes, absolutely, and especially if you expand it beyond just the US and the United Kingdom. If you look at what your Government have suggested—the D10 of 10 great democracies, with the G7, India, South Korea and Japan combined, and of course throwing in other European nations as well, but with the United States and the United Kingdom at its heart—I have no doubt that we have the talent, the productive capability and the innovative and entrepreneurial spirit to develop 5G technologies, both software and hardware, that will far surpass in quality, performance and price anything that China produces.

- Q81 **Mr Francois:** Lastly, do you think it is realistic, given the economic pressures of covid, that Congress would help finance that or at least help to pump-prime it?

Senator Tom Cotton: There is no doubt about that. Again, this would be an example of swallowing camels and choking on gnats. There is legislation in Congress that proposes spending a few hundred million dollars, a billion dollars, on helping to promote that kind of technology. We would, of course, call on our partners to help pitch in to the kind O-RAN Alliance that your Government have suggested, so that we are all in the boat rowing in the same direction. However, in the same way that it would be penny wise and pound foolish to short-change our military, it would be penny wise and pound foolish to short-change the opportunity we have in the months and the years ahead to try to develop an open 5G system that can overcome Chinese technology.

Chair: Thank you, Mark.

- Q82 **Sarah Atherton:** Senator, I am interested in exploring your initial reaction to the UK Government's decision to allow Huawei continued presence in the 5G infrastructure.

Senator Tom Cotton: Like our Government's stated reaction in January, it disappointed me. I understand that you face a different kind of situation than do we, because of the legacy networks you have—the 3G and 4G networks—that use Huawei technology. I do hope that as the Government refines its decision, if it does not reverse it outright, it will mitigate it by minimising the use of Huawei technology, putting it on a shorter



timeframe, limiting the expansion of the 5G network and taking the steps we have done to help wean 4G and 3G networks off Huawei's legacy technology.

I have seen media reports that suggest that could happen as early as 2023. I would welcome that—I would welcome you doing it even earlier. I am a bit mystified about why you would spend the money to build out a 5G network using one kind of technology only to tear it out three years later. But again, we will continue to observe and work with your Government and the decisions they take to try to ensure that our alliance remains as strong as it always has been and that we are also creating the kinds of alternatives that Mr Francois and I were just discussing for the rest of the world.

Q83 Sarah Atherton: If the Government do change tack and reduce Huawei to zero by 2023, as you just said, would that be enough to mitigate your concerns?

Senator Tom Cotton: It obviously would in 2023, but remember that many of my concerns are not specific to the United Kingdom. To go back to legislation that we discussed earlier about F-35 fighters, we have got to make a decision about deploying those to many different countries. Obviously, if you no longer have Huawei technology in your network, then F-35 fighters could be based in your country under my legislation. That does not mean that I would drop my legislation, because my legislation is not about the United Kingdom; it is about Huawei and the threat that Huawei poses to our airmen and our aircraft. But I would welcome that decision to go to zero by 2023, and I would urge you to try to do so even sooner.

Q84 Chair: This is my final question, if I may, following Mark Francois's question. The reason we are in this situation is that we have relied heavily on the commercial sector to provide the answers to 5G while China's response has been very much to state fund their commercial sector to provide the high-tech and cheap solutions which they are now able to sell with abundance around the world.

Congratulations on your SpaceX Dragon connecting up with the space station, which is a great example, like Apollo, of a marriage between the commercial sector and state funding, but clearly the parameters for 5G go way beyond any individual nation. Would you agree that there is scope for the Five Eyes community to invest, putting money up front and working with the commercial organisations to create that international, secure, established network for us to move forward with, so we can actually replace Huawei far faster than perhaps even our Government is intending to do?

Senator Tom Cotton: Yes, I think that is a great opportunity for our nations, and in the long run it will probably be exactly that kind of open network technology that allows hundreds or thousands of companies to compete. Rather than putting all our eggs in one democratic alternative—a company that we hope will be able to compete with Huawei and ZTE, which is what the Chinese Government has done with its massive



HOUSE OF COMMONS

subsidies—we can try to develop the kind of open infrastructure that will allow any company in our country or your country to compete and build this cutting-edge technology that our countries will be so vitally dependent upon.

Chair: Senator, thank you very much for joining us today. It is reassuring to hear your determination to continue furthering the special relationship. I hope we have also proved that when there are differences of views, we are able to express them freely and work through them. We face a very challenging time internationally, and I think the more the US and the United Kingdom can stand up and show international leadership, as we did during the second world war in creating the bedrock of organisations for that period, so again must we work together in this difficult time now.

Senator, on behalf of the Committee, can I say thank you very much for joining us this afternoon?

Senator Tom Cotton: Thank you all.

Examination of witnesses

Witnesses: Brigadier General (ret.) Robert Spalding and Mike Rogers.

Chair: I am conscious that there is a vote in a few minutes, but we will continue. We may lose some Committee members, but I am delighted to welcome Brigadier General Spalding and Mike Rogers, who I hope are now with us virtually. It is good to see you both, sirs.

Brigadier General Robert Spalding is a former air force general and previously senior director for strategy for President Trump. He is now senior fellow at the Hudson Institute. Mike Rogers is formerly of the US Army and the FBI, and a former Congressman for Michigan. He now writes extensively on cyber-intelligence and 5G specifically in connection with Huawei and ZTE. He is chairman of 5G Action Now. Sirs, you are both very much welcome to our Committee hearing. We are very much looking forward to hearing what you have to say. Because of time constraints, we will go straight into it.

Q85 **Mr Jones:** Welcome, gentlemen. Could you give the Committee an overview of your concerns about Chinese involvement in the telecoms sector?

Mike Rogers: First of all, thank you very much, Chairman and Committee members. I am honoured to be here. I would like it in person, because I understand after the Committee there is a chance for a pint along the way. I can't wait to get back for that portion of the Committee testimony. Thank you again for that special relationship. I, too, am a complete believer that we are better together as we move forward in this uncertain time for this great power competition that is about to be on us.



HOUSE OF COMMONS

I would say that my concern with the Chinese Communist party's heavy involvement in the telecommunications business is really in three buckets. There is economic security, so think about IP theft—trillion dollars of intellectual property stolen. That means economic prosperity for the future could be lost, and likely is lost. There is the fact that they put themselves in a position for economic extortion. We have seen that most recently when Australia came out and said that they were going to investigate the origins of covid-19, and the Chinese Government came back and said, "Well, that would be great—so maybe the Chinese won't be interested in drinking Australian wine or eating Australian beef". Clearly, when you empower them in an economic sphere—and data is that next big economic sphere, in 5G—we have something to worry about, for sure.

National security is another bucket. Think about Government secrets, military secrets, diplomatic secrets, their continuing targeting of US military readiness, technology, capability, all of that—and intention, by the way—is all part of that bucket of national security that we worry about, including the fact that they can turn things off. So, if you get into a conflict, if they are controlling networks in Great Britain, the United States or anywhere else, they would have the ability to shut certain parts of the network down. You can imagine the confusion and chaos that might cause for anybody that is taking the chance to use this gear.

The last bucket is personal security—think about personal data. I heard you talk to Senator Cotton earlier about privacy and privacy of data. That is going to be incredibly important. This is a nation that has set up a credit scoring system to get every piece of data—in some reports, as many as 2,000 points of data on each citizen—and then score them and use that against those citizens if they have ill feelings towards the Communist party in China. As a matter of fact, in the last couple of years, 6 million Chinese citizens were prohibited by the Government from buying tickets on aeroplanes and trains because the Chinese Communist party deemed them not worthy of having that right within their country. Remember, these are the same folks who are talking about trying to get hold of our networks and the data that flows over them. As a cyber-security guy, I can tell you that if I can touch your data, I can get your data. Access is everything, including in the intelligence space.

I look at those three buckets of why I am concerned and, going forward, why we ought to worry about this together. I hope the Prime Minister, as he has talked about, is maybe rethinking his position on Huawei. I hope that he reconsiders and that we will have at least some time today to talk about the issues why even further.

For my last bit of evidence, I am going to read some of the charges that have been brought against this company. These are US charges but other countries have experienced the same. This is against Huawei: racketeering, conspiracy to steal trade secrets, commit bank fraud, conspiracy to wire fraud, bank fraud and wire fraud, conspiracy to violate the International Emergency Economic Powers Act and effective trade secrets. The list goes on: obstruction of justice and other things. If this



HOUSE OF COMMONS

were a French company, a Russian company or a US company that came to Britain and said, "Because we are big and important, we think that you should give us a piece of your market; we should guarantee that I get a percentage of your market," what board of directors in the world would look at a company with this track record and say, "Yeah, come on in, we will make accommodations for you," based on what we know about their behaviour in the past?

Just a couple of quick newspaper highlights: "China stifles foreign internet to control coronavirus coverage", the *Financial Times*; "European mobile traffic mysteriously routed through China for two hours", *The Independent* in the UK—by the way, as a cyber guy, it is not mysterious; we know how this works and they did it on purpose—"China systematically hijacks internet traffic: researchers", the *iTnews* in Australia. By the way, what they found was that any time there was a trade negotiation or something of importance to the Chinese Government, traffic got routed through China.

These are the folks who had control of networks using that access to those networks to do things that would not be in line with our values. That list is pretty long and I could go on for a while. That gives you, at least, an understanding of why so many of us in the national security space are so passionate about making sure we get these decisions right.

Q86 Mr Jones: I agree with you on the threat from China in hacking and in some of their clear examples of stealing intellectual property from companies. I would be interested to know about the relationship between the US and China in terms of some of these technologies, because a lot of it is being funded by investors from the United States investing in Chinese companies. You say that there is an ability for Huawei to be able to turn off the network. Could you explain how that would happen? I struggle, having had extensive briefings on this, to understand how you would do that when you do not have direct control of the network in each country.

Mike Rogers: It would be pieces of the network. The thing about 5G is that people say, "Well, we can protect the core." The interesting thing about the 5G development of technology is, if all of that is in the core, 5G is not functioning properly. It is about pushing the security to the edges—to the end users.

When you do that, it gives the ability— If I am doing any multiplexing in that system, meaning that if I am moving data, interpreting data and sending data somewhere—we would know it as routers and other pieces of equipment—then, if I am doing the patches on those pieces of equipment— By the way, the vendor operators do the patching: every day, lots and lots of administrative functions go over into these devices to make sure they are functioning properly. They get updates. They get the latest and greatest technology. And if you have the ability to do any administrative function, you have the ability to disrupt that function, because you have access to those units. It might not be that your whole network goes down, but what you could do is jeopardise certain parts of



your network. If you know they are interested in economic extortion—we have watched the Chinese do this—I think you would have to be concerned about their ability to go in and make things really difficult or even just slow it down so it is overwhelmed.

Q87 Mr Jones: But General, you do not need access to the hardware to be able to hack into a system. In terms of the example you have just given, a network vendor or operator would know if data was being taken out of part of its network and be able to stop it. I think the bigger threat is from hacking and some of the technology that the Chinese have invested in, in terms of military and other, to steal secrets. That does not necessarily need the hardware. That is a hacking issue, which they have trained very extensively on.

Mike Rogers: I am not sure if you want the General to answer; I was just a lieutenant in the army—

Chair: Let us allow the General to answer. Robert, can I give the floor to you?

Brigadier General Robert Spalding: These are all great issues and good conversations. The challenge that we have is understanding what 5G is. Really, when I hear the telecom industry talk about it, they are not really talking about 5G. 5G is not really about faster speeds. It is about building an industrial internet that provides for automation, self-driving cars, industry 4.0.

The challenge that we have today is threefold. First, there is the technological challenge. We built the current mobile internet on fundamentally the same data model that the internet was built on, and that is an open data model. To the point about, “If you’re in, you’re in,” that is the challenge with the data model. That turned into a business problem for telecoms.

What happened with the open data model is that the tech companies from Silicon Valley came over the top and monetised user data. When they monetised user data, they took all the value out of the system. In the United States, we spent \$250 billion building these networks and then the telecom industry wasn’t paid back for it. On top of that, what you had over the course of 10 years from 2007, when the iPhone came out, was a complete change in the global economy, going from an industrial economy to an information economy. AT&T was top five in market cap in 2007; in 2018 it was nowhere to be seen. You have instead Facebook, Amazon and Google.

What you have in addition to the technology problem and the business problem is a policy problem, because we haven’t caught up to the fact that national security has fundamentally shifted from the traditional battlefield arena to right in our own midst. We are talking about social media influence and the undermining of our collective economies, and most of that is surrounding the use or misuse of data.



HOUSE OF COMMONS

This is what the Chinese Communist party figured out. The way they do this is to first create a moat around their population to ensure that they can't be attacked, and then have the freedom to attack others by deploying the network. How do they do that? Well, they know that there's a business problem in the telecom industry, so they take Baidu, Alibaba and Tencent—their Silicon Valley tech company examples—and they pool the enormous amounts of money. Alibaba alone made \$38 billion last November Singles Day, on 11/11—in one day. They pool that money and they subsidise the deployment of the network, because they want access to the data.

If you listen to Kai-Fu Lee, their leading artificial intelligence researcher, who says, "We are to data as Saudi Arabia is to oil." Their goal is to, behind that firewall, collect and then monetise that data. And that's not just for the economic dominance of China; it's also to influence. If you look during coronavirus, 40% of the posts on social media are coming from bots. I would venture to say you are probably seeing the same thing going on with the riots that are happening in the United States right now. They have learned, and learned very well, how the internet can be used to influence populations.

Chairman Rogers talked about how they are doing that in their own society, but they are also figuring out how they do it abroad by using Huawei as one of the avenues for it. It's not just Huawei. Huawei is a member of 3GPP, which is the industry standards-making body. If you look at the security of the 5G network today, across all the tech stack of 5G, there are 800 write-ups in front of 3GPP for security—3,000 technical vulnerabilities just on the 5G network stack. And if you look at all our networks—not just yours but ours—they are networks that are built on 2G, 3G and 4G, so they are adding 5G radios to an already insecure network with an insecure tech stack.

We are talking about the right things, but we have to understand the problem we face. It's not a problem that's unique. It's one of those where a technology has become, in front of our eyes, dual-use technology in terms of its being used to undermine our economies and our societies. And we do not have the means to stop it, primarily because, in the United States, we created the Global Engagement Center. This was supposed to counter influence over the internet, but what we have found is that the Global Engagement Center and State Department don't have the authorities to collect data so that they can understand the influence that's going on. Right now, Carnegie Mellon is one of the universities—there are others around the country—that are trying to make sense of the influence that's going on on our social media networks. Quite frankly, our intelligence community is sidelined because of our own law. This is what the Chinese and the Russians quite frankly figured out, and I think they have harnessed it quite well for their own ends.

Chair: Thank you for that. Richard Drax.

Q88 Richard Drax: Good afternoon, General, and Mr Rogers. Before I ask you my question, can I pick up on a question that I asked our Prime Minister



HOUSE OF COMMONS

recently? The French are apparently doing a root-and-branch review of every single defence supplier or provider in their country, because there is evidence, as I understand it, that China is buying up all companies going bust during this pandemic. Do you have any evidence of that happening in America, and even if you don't, are you also checking your supply lines so far as the defence industry is concerned? General Spalding perhaps would be best placed to start on this one.

Brigadier General Robert Spalding: This started back in 2014, looking at the industrial base. Not only are we losing tech start-ups that would be considered dual-use technology, but we have already seen the erosion of our industrial base. The main challenge that we have as a country is that we do not have an industrial policy to speak of that really ensures those critical things that we need to ensure that we have made either in the United States or in the country of an ally.

Q89 **Richard Drax:** Coming to my question why the United States does not have a global market-leading provider of 5G, I think you have answered that in several ways, not least in the inability to collect data. If that is the case, what is the United States doing to increase its capability in this area?

Brigadier General Robert Spalding: Unfortunately, we are not doing enough because the need remains. The chief problem in the industry today, if you want to deploy 5G, is that, first of all, we are not deploying it in the manner in which I talked about, which requires data security and data sovereignty in the network, and really an industrial, more of a military-grade network so that you can protect and prevent the hacking of self-driving cars or remote surgery.

That is No. 1, but the thing that is really preventing us is that we not have enough volume of production of the radios to actually get us down to a price point such that you can deploy it easily. The reason we do not have that is because none of the telcos are buying a lot of radios. The only ones that are deploying a lot of 5G radios today are the Chinese. The South Koreans did in South Korea, but the Chinese are really getting their production flow in for their radios, so they can actually get a price point in addition to what they are subsidising. We are not doing it because our telcos are not buying enough radios, so if we want to really get after this, it is really about having a major project that bumps up and gets us in the production flow.

Mike Rogers: May I make one quick point on this? We often talk about our Five Eyes relationship—our Five Eyes partners—and the Brits are certainly very high on that list. Here is where I think we made a mistake. The general is right on industrial policy. We are having those debates domestically. What does that look like? Should the Government do it? Should the private sector do it?

I have some pretty strong thoughts on that, but I think we can help even companies that have the same values. If you look at Ericsson and Nokia, which are really in your neighbourhood, so to speak, and which have the



same kinds of values that we would appreciate in the build-out of these networks, they cannot compete when a company like Huawei is so heavily subsidised by the Chinese Communist party on two fronts. They subsidise the research and development, which takes the cost almost off the shelf for pricing—to price their products. That is No. 1. No. 2, they finance deals with zero-interest loans or no loans at all, just by financing deals and allowing them to take that equipment to places where the deal is so good that no western company or no free market-oriented company can even compete on the price.

That, by the way, is exactly how I got on to the Huawei-ZTE problem back in 2010. Someone walked into my office as chairman of the intelligence community and said, “I don’t know if this is a problem or not but somebody wants to build”—I think—“13 towers with all the gear on it, and it cost me less than two towers for the nearest competitor.” I said, “Boy, I don’t know much,” and I may have had to take my shoes off to count that high, but I thought that something doesn’t smell right here.

That kicked off this whole investigation about how they were crushing the private sector, free market, competitive companies who have the same values as we do by doing these kinds of deals that no one could compete with. This is where I think we have an opportunity to step in and help them, through EXIM Bank and other things, to say, “We’re going to at least allow you to be competitive with a Chinese company.” Right now, it is pretty hard to do that when the Government is supporting their efforts.

Q90 Richard Drax: I hear you, Mr Rogers. We have heard many of the answers that you have just given from witnesses who have given evidence to us before. My question to both of you is, bearing in mind that this is such a serious issue—I think we are looking at the future of the defence of the west; it is as big as that—what is the Government doing about it?

Mike Rogers: I can say this. The US Government today is having some debates on what that looks like, but on the first step that they did I know they took a lot of heat for this. The Trump Administration has been excellent in saying, “We’re gonna finally confront Huawei gear and purchases, and one of the ways that we can do that is by saying, ‘We will not allow them here.’” And that hurts. It deprives them of revenue. It sets the security standard of what we think a security standard should be for these companies. Huawei would not fit that within 100 miles. So that was the first step, and I think it was a concrete step.

I have met with our Canadian and British friends on this notion that you can be a little bit pregnant with Huawei gear and everything will be okay. I just don’t believe that. It also hurts the grand notion whereby if they are a collection platform for the state of China and they are illegally subsidising, using it to illegally steal intellectual property, and using it for espionage purposes, in addition to what its function is, we really should not allow them to be anywhere, so the most immediate thing we can do is just to say no: “Because you don’t raise to these standards, we can’t let you in.” If they want to go back and change the way they do business, we should



HOUSE OF COMMONS

think about it, but they are not doing that because it's in conflict with their data dominance by 2025.

Q91 **Chair:** Thank you for that, Richard. The focus of this study is not just to nudge our Government into the wider thinking, but also our parliamentary colleagues. You talked about a wider debate. It still feels as though it is not resonating with the general public. Are we missing a Sputnik moment: that point in 1957 when America woke up and recognised that the Soviets were far, far ahead and there needed to be an invigorated effort to not only catch up, but overtake? Do you feel that we have reached that moment yet, or is it yet to come?

Brigadier General Robert Spalding: I think it is yet to come. You can see the signs, but if you are not looking for it, it is very difficult to tease out the impact to our democracies and to our economies of what has been essentially going on over the last 10 years. The challenge is really describing it to people. Most people don't understand the technology, they don't understand the business, and therefore they don't understand the foreign policy and national security policy implications. I am not talking about just the general public; I am talking about national security professionals themselves. They are totally comfortable talking about the land, the sea, the air and space in terms of the threat to our societies, but, in terms of what the internet has, it is very difficult in terms of that group to really understand it or articulate it.

Mike Rogers: Just to add to that, I am a little more optimistic only because of the tragedy we are in now with covid-19. People are seeing the stresses on what people thought would be normal behaviour to share masks, personal protection equipment or medicines, but what we found with the Chinese Communist party is they went internal. They hugged around it and said, "We'll share it with who we want and we'll use it as a weapon on people we have differences with." That I think is going to wake up the American public on a reliance on a supply chain of critical materials, and I think we can slide 5G into that in the future. Do you really want to be dependent on the Chinese Government when everything goes wrong? My argument is: probably not.

Q92 **Chair:** Thank you. General Spalding, you wrote a memo to your own Government about Government build out on 5G networks. Have you had any response?

Brigadier General Robert Spalding: I think there has been a positive response in some quarters. The problem that we have, again, is the same problem that you and other democracies have: the entrenched interests in the telecom industry don't want to see change and, quite frankly, they are not capable of deploying the type of network that I think we are trying to get to in terms of promoting industry 4.0. We are in a place where, because of convention and because of our established business models, it is very difficult for us to break out of it. It is one of those things where Government actually has to take a leading role. I just look at British Telecom as one example. There is a requirement for British Telecom to provide services to the people of the UK, but there is also a definite need



HOUSE OF COMMONS

in the UK, going forward, for an advanced AI platform for the automated things of the future, which is not British Telecom's business right now. Ultimately, you cannot take that network and modify it to do those things. You have to build an entirely new network, and that is the challenge that we all face. All of these use cases and applications that we are talking about will never come to market unless you build the network, because we are talking about a new type of network—it is not just communications but computing, and it needs to be done securely.

Q93 Chair: Thank you for that. I will just explain that we have lost a couple of colleagues. Ironically, we are having a vote on how we should vote—the virtual process of voting, or whether we should be here in person or not. That has clashed with our Committee, which gives an illustration of the challenges that we currently face. I am conducting my own little rebellion against that by staying with you and focusing on my Committee work. I am glad to see some of my other colleagues have done the same.

I want to focus on the actual companies themselves, and what is on offer there. If you do not want to use Huawei or ZTE, who is actually out there? From the British perspective, you have Ericsson and Nokia, which you will be very familiar with; NEC, which is Fujitsu-based and focuses on Japan; and Samsung, in Korea. In the United States, what companies are now advancing your own 5G capabilities, and are they now gaining any state sponsorship to upgrade their abilities to overtake what Huawei or ZTE actually offer?

Brigadier General Robert Spalding: There are a couple of companies—JMA and Airspan—that produce 5G radios. JMA is more of an OpenRAN company. Airspan has more proprietary equipment, kind of like a Samsung, but in very small volumes. The problem, quite frankly, is the lack of real investment in 5G. Those are the radio providers.

On the core provider side, a mix of companies have been selling to the telecom providers based on a service-based architecture. Altron is one. Greenwave is another. Microsoft just bought Affirmed, which is another software core based on a service-based architecture. All those are essentially building traditional telecom software core. Right now, looking at the core business, there are not a lot of what I would call enterprise-industrial internet providers among the software providers for the network equipment.

Q94 Chair: But none of these, in the spirit of that Sputnik moment, are receiving state funding to expedite and advance their offering.

Brigadier General Robert Spalding: Not yet.

Q95 Chair: It seems very late in the day, given the length of time that this debate has actually been happening for. I agree with you: that Sputnik moment has not come. You mentioned the OpenRAN policy, or the programmes on offer. There was talk of a coalition forming on OpenRAN. Can you expand on that, and on what is happening on that front?

Brigadier General Robert Spalding: There are companies coming together in OpenRAN. At the end of the day, the problem with OpenRAN,



HOUSE OF COMMONS

just like I stated, is the lack of investment coming from the telecom industry to really accelerate its deployment. That being said, I think you are going to see OpenRAN 5G radios in the market by the end of the year. Again though, if you want widespread deployment, you have to get into production flow, and in order to get into production flow, we are talking volume orders. We need to see an order for 10,000 radios, not an order for 10. That is the challenge that we face today. If you really want to make your country competitive for the future, you will have to look at this more as a national strategic investment, and somehow stimulate that with policy.

Mike Rogers: Just quickly on that, the ORAN group is coming together. There are some interesting conversations from the US Administration with companies that are producers—even those that are currently in the business, such as Ericsson and Nokia—about how that plays out in the future. I am pretty optimistic about that.

There has been a little bit of a difference in debate on how we get there. I have been for the US Government trying to get out of the way. One of the ways that we would do that is by clearing spectrum—they call it the Goldilocks spectrum; it is sub-6 MHz. Unfortunately, that has been clogged up for a long time. We finally got our Federal Communications Commission to agree on an auction. Chairman Pai has done an excellent job to open up that spectrum, help clear it out and put it up for auction. I think that you are going to get lots of investment once there is certainty. Right now, there would not be enough certainty, based on what spectrum we have available. For a long time, that has been a circular firing squad for the United States. We have often talked about why we do not invest. Well, we can't invest because we cannot get in and have no certainty. We have no certainty because we have to leave the spectrum to someone else. That is starting to get cleared away in a way that I think will allow the United States—not only through the ORAN initiative—to make those boxes dumb. There will be no intellectual property of value, meaning that that can be a commodity. I am not even sure that I care where it is produced, because the real value will be in the software, the virtualisation and the network slicing that lays over that gear.

If you open radios, clear out the spectrum and allow US companies to bid on that spectrum in the United States, you will get AT&T and Verizon interested, and all the big players—companies such as CenturyLink and others—will now be able to participate in a way that they could not before. I am not as pessimistic. I do think that we are a little behind, but once you unleash the hounds of American innovation, I say, "Look out!" That is the way that we are not only going to be able to match the Chinese, but beat the Chinese in the future.

Brigadier General Robert Spalding: I will just say that when you go back to the last industry disruption, it was based on the mobile platform as the compute. Of course, the 4G network was the pipe. In that case, what you could do is rely on consumers to buy the equipment—to buy the platform essentially—and it was consumer adoption that really drove that



industry disruption. What we are talking about here with 5G is on the infrastructure side. Consumers do not drive infrastructure investment. That is done at the enterprise level. So we are looking at enterprises that need to invest in a technology for which, quite frankly, they have not determined the business model. This is really the chicken and egg problem: how do you spur investment in what is really an enterprise investment and not a consumer purchase?

Mike Rogers: When you look at the sheer number of sensors and what that will mean to enterprise productivity increases and profitability, that will drive this train—that is the other side of it. There are companies out there now that are looking at secure 5G and how they protect the core and the control plane in 5G. To me that is exciting; there is going to be some opportunity here, but we have to clear out the underbrush to get there.

Q96 **Chair:** Can I ask a little about greater collaboration between western vendors themselves? That seems to be the challenge. In relation to that, you understand the British set up. There has been pressure from the United States—quite vocal, open pressure; not least from Congress and so on—that Huawei should get out of our 5G conversation. But you are aware of how embedded Huawei is in 3G and 4G. Is it realistic for this Government to be able to make a commitment to unpick that in the next couple of years?

Mike Rogers: I happen to think that that is possible, but it is a commitment and will not happen overnight. We are working through this in the United States. We have companies that have Huawei gear in old legacy systems, and with mergers that have happened in the last decade, they have picked up quantities of Huawei gear in their networks. It is expensive to replace; no doubt. So here, the US Government are considering helping fund—they call it rip and replace—so they are going to help these companies rip and replace. I think that is all but certainly here coming up in the fall and they are going to promote a mitigation plan for these companies to get out of it.

We would like it to happen fast—it is probably not going to happen as fast as we would all like. I think Britain can do the same thing; it gives you an opportunity to come up with networks. I think it's kind of exciting. In order for 5G to work, by the way, you have to have a functioning 3G and 4G—it's just the way it works. So can you come up and be creative on what happens next on these networks that helps you mitigate the problem? I know the answer is yes; there is some great technology on the horizon, and we all want to be together on it. I do believe that maybe just beating our good friends the Brits over the head is probably not the best way to go about this; it is better to invite someone to the dance, and I would hope that we would engage in this in invitation to the dance, because I think we can be a pretty powerful team on Huawei.

What worries us, and worries me, even as the Chairman and in the security work that I do now, is the message that it sends if the UK just says, "Yeah—you know, whatever; our guys say it doesn't really matter, therefore it really doesn't matter." That's dangerous, and it is going to do



HOUSE OF COMMONS

make people make decisions based on a heavily subsidised Chinese Government product that has ulterior motives because it is cheaper. So I worry about that a little bit, but I do think that we ought to find our way forward on this, and I think there is a way to do it.

Q97 **Chair:** General, did you want to comment?

Brigadier General Robert Spalding: Just a little bit on the rip and replace. We are finding some issues in terms of the adoption by the rural operators because, frankly, they don't want to pause service and deal with the challenge—with that. That is one thing to consider when you are looking at what your policy should be. I favour a standalone 5G network that is built securely, that is built alongside your existing networks, because it allows you to take a clean sheet of paper and design a secure network from the ground up. I think that is the only way you are going to be able to deploy the network of the future, because I think if you are trying to do it the other way you will constantly have security issues.

Chair: Thank you for that.

Q98 **Martin Docherty-Hughes:** Good afternoon, or good morning, depending on which part of the United States you are in. Mike talked about buying cheap. We have an expression where I am, in Scotland: "Ye buy cheap, ye buy twice." Quite clearly, that is where the United Kingdom of Britain and Northern Ireland is heading right now. My question, which I think you have already answered, is: how can western Governments work together to prevent high-risk Chinese vendors from gaining a foothold in our networks? I suppose that is, you don't buy cheap and you don't buy twice; you work with our key allies. Would you agree with that?

Brigadier General Robert Spalding: I agree with that 100%. Chairman Rogers talked about rip and replace. I would advocate making a bulk buy of radios, so that when you go to spend that money to invest in that, those radios are now in production flow and you get much more bang for your buck.

I think we could really do a good job if the Five Eyes got together and really stimulated production on that, because once you do that, the investment will go a lot farther, but until we get that kind of big purchase— Right now, you are relying on the onesie-twosies in world markets, buying radios.

If you were to basically stimulate a large buy for the five of us, now you have a pool of radios that you could potentially really use to maximise your replace.

Mike Rogers: I agree completely with General Spalding.

I would argue again, if we all came together, as the Five Eyes, and said, "Here's the security standard for anybody that competes in any one of the Five Eye countries," that bloc would lead to the bulk purchasing that the general talked about, and it would prevent Huawei and ZTE making the argument—because we know what they are doing; they are going to make



the trade argument with our friends in Britain; they are going to argue, "There is a cost to this; if we can't get in your market, we are going to find ways to punish you." My argument is, okay, we will get around that, by agreeing, as the Five Eyes partners, "This is the security standard." And by the way, that standard will be adopted by others, because they will know the care and concern that we would go through to make sure we got it right.

I like that approach, so that you are not buying twice. If you buy Huawei, you are going to buy it twice. You are going to have a problem at some point. You are gonna regret it at some point; it will happen. And then you are going to have to figure out how to get out of it. I think that first start could be, "Let's band together, create these requirements." As the general said, let's buy in bulk; let's figure out a way that we can buy these networks in a way that drives down prices and helps consumers at the end of the line.

- Q99 **Martin Docherty-Hughes:** Perhaps we could take that a wee bit further, rather than just Five Eyes. The terminology, I think, is "western vendor of 5G". I prefer the terminology "5G vendor from a liberal democratic state", because it is not just the west. Who would you invite to the dance, Mike, to create a more robust 5G network for liberal democratic nations?

Mike Rogers: I don't disagree with you and I don't disagree with your description, but the problem is that we have a time crunch. Here are the five countries that we have very deep security relationships with. We can sit in the room and in SCIFs—behind the curtain, as we would say—and say, "We're going to share what we know about how the security services of China manipulate these networks and companies." We can have that pretty quickly.

It is not that we don't trust other nations, but, as you know, the challenge beyond Five Eyes is that we don't have the length and depth of relationships and security. Each country has a bit of a different view about intelligence and how we share it. My argument is that if you want to do it fast, do Five Eyes first and say, "Just for us, we are going to set the standard. We would love to then invite people in to join us in the standard, or at least broaden it out." All those countries across Europe would be interested, in my mind, and then you look at the countries in Asia that are under the foot of heavy Chinese influence operations and other things.

- Q100 **Martin Docherty-Hughes:** On that, Mike, you talk about the depth of relationship through Five Eyes—Australia, New Zealand, Canada, the US and the UK—and I totally agree with that. I totally get it, but are we effectively saying that there is no way in which we can invite others to the dance? In another roundabout way, are we saying that we don't have a robust, long-term, in-depth relationship with the French Republic, for example?

Mike Rogers: No, but the reality part of an intelligence-sharing arrangement is that there is a reason why there are five. These are the nations that have come together. We understand and participate at levels



HOUSE OF COMMONS

candidly. It would take your breath away how open these countries are with certain really sensitive things. I think it is a really great thing. We don't have the same relationship with the French intelligence service, but we have a great relationship with it, and with the Germans and Poles, for that matter. But on the technical side, they don't raise to the same level.

That doesn't mean that those countries can't participate; I would encourage them to do so. The bigger this thing is, the better it is, but if you want a quick solution of setting what a security standard looks like, because we have this incredible sharing relationship, I would start with the Five Eyes. It is an easy meeting to convene. If it gets bigger, you have to go through all the nuances: "Can we share this? Can we not share that?" In the same way, the Brits don't share some things with the French for whatever reason, and we don't question that. That kind of thing would have to be worked through.

Again, I don't disagree. I would love to have everybody at this party, but in order to get the party started—a famous American singer said that at some point—we have got to have that Five Eyes relationship working up front. That is the way I would do it. I'm sure other folks have different opinions.

Brigadier General Robert Spalding: I would totally go off that theme and look at interoperability and the need for our forces to operate across one common platform. So Five Eyes, absolutely, and NATO might be another idea. NATO, Japan and Five Eyes—between those three groups, you could create a very strong buying coalition for a secure 5G network. All the forces need them—all the bases need them—and this would really stimulate the deployment of those alternative military grade secure networks.

Q101 **Martin Docherty-Hughes:** Robert, the next question is for you specifically, but maybe Mike will want to come in on it. Could liberal democratic vendor 5G provide an alternative to the Chinese digital silk road for other countries—some would use the word "developing", but that is not a term that I find fit for purpose in the 21st century?

Brigadier General Robert Spalding: This is a far easier challenge, but for the United States it is one that we have been struggling to meet. That challenge is getting USAID, the Development Finance Corporation, TDA, EXIM and all of these things aligned around a more strategic application of development finance, and bringing in other organisations such as JBIC. This is a thing where, among the same group of countries, we could come together and be much more forward thinking.

I call it building rather than breaking. In a lot of ways, it is like the Marshall plan: using our combined efforts to drive development in these economies in a way that also promotes democratic principles, human rights, civil liberties and free trade. That is something that needs to be done, but we do not act strategically in that way. We typically tend to focus on the military aspect of our alliances instead of on the building part of our collective economies, and, quite frankly, we do not get the private



sector involved. Many in the United States do not get involved outside our borders with EXIM, USAID and DFC, so this is an area where we could change the way we collectively work and promote our collective security.

Q102 **Martin Docherty-Hughes:** Just in terms of Europe and North America—I include the United Kingdom in Europe, because it is part of continental Europe—do you think we have lost our technological dominance? I am not asking whether that is a good thing or a bad thing, but it does have—

Brigadier General Robert Spalding: No, no. This is actually what I found when I was working in the White House. The problem is that the technological dominance has shifted out of the telecom industry into the defence industry. Whether you are talking software-defined radios, antennae, software-defined network computing or security—all of those pieces—we have been pouring money into defence development, and they have not been brought to the commercial market because of the market forces I have described.

For example, we used to have Bell Labs in AT&T, which was getting money from the Government to do basic science research. Of that basic science research, the stuff that still remains is in the defence primes, so we have a lot of very advanced capabilities that end up either being deployed as a one-off in the military or put on a shelf after development. It is just about bringing that into the commercial sector, recognising telecom as a dual-use technology and then deploying it in the proper way.

Martin Docherty-Hughes: Mike, do you want to add anything to that?

Mike Rogers: I do not think we are losing. We used to be so far superior that we always used to count on our decade-long gap in intelligence with our nearest peer adversary, and that is just closing. It does not mean that we are not knocking this thing out of the park; candidly, I think we are.

My biggest pet peeve is when people say, “China’s beating us in AI.” The reason their algorithms in AI are performing at the level they do is not because we aren’t where they’re at—I would argue that in many places, we are ahead of it—but because they do not have the same concerns about privacy as us. The pools of data to which we can apply our AI algorithms are pretty small compared to what the Chinese do: 700 million or 800 million people, with 1,000 or 2,000 data points per person. Those algorithms get better as they run on bigger databases, so even there, I push back a little bit and say, “No, we’ve got some issues. We’ve got to get out of our way, we’ve got to work together as liberal democracies will do, and we will get over our small differences.” I always argue that they are smaller differences than with our adversaries.

I think we are going to be okay, as long as we are paying attention to it and trying to get ahead of it. If we just let it happen to us, you are right: we will be standing in the dust, wondering what in the heck happened. However, as long as we understand that we have these challenges—that we have to get out of the way, empower the private sector and use it with the Government—I think we are going to be fine. On the development of



5G, remember: if we can get to open-source radios and get all the spectrum figured out, the good news about what happens next is that we are going to own what lays over those software-defined networks. That is an area where the United States and our allies are far superior to where the Chinese are today, and that is going to be a big part of why 5G is successful, so we ought to continue to promote that as well.

Q103 Martin Docherty-Hughes: Can we move beyond the access point in terms of the technology around 5G, and then look at issues around ownership of data and gaining accurate, timely and high quality data? Some people would say that is where the wars of the future will be won, in terms of gaining knowledge.

You also talked about AI. AI itself—I suppose everyone keeps forgetting the acronym—is artificial. It is initially being pushed by a human being for a specific purpose. I am just wondering, are we winning the battle around access to accurate, timely and high quality data? I don't know, General, if you have got some points on that as well.

Brigadier General Robert Spalding: Our challenge is, again, the open data model that Chairman Rogers just mentioned. The challenge is that the authoritarian regimes have figured out the power of that, and it really lies in the aggregation of data. The more data you have, the better your AI is. I think one of the things that democracies have the ability to do is not listen in on their citizens. What I am talking about here is pervasive encryption across an AI platform that enables the preservation of privacy but then, at the same time, allows for the use of those algorithms in ways that promote our principles. This is not something that, quite frankly, the Chinese Communist party can compete with, and it would really become a competitive advantage, but it really requires us in the free world to change our focus from an open data model to more of a closed data model that is more consistent with GDPR. GDPR doesn't work, because the world is still on an open data model. That requires a change in how we treat data on the network. If we change the way we treat data and we actually make that owned by the individual creator, then it becomes much more powerful in terms of innovation and participation.

Q104 Martin Docherty-Hughes: Sorry to interrupt. I know we are conscious of time, Robert; but on ownership of data, the Chinese are very good at using distributed ledger technology—their version of it—to find out how good a communist you are. I am just wondering whether you think technology like distributed ledger technology, within liberal democracies—perhaps if it is closed distributed ledger technology—can be utilised to create an element of trust around the ownership of data, because there is a huge element of disinformation and nudging of the narrative. We look at, for instance, profiling, even in liberal democracies, by those who own the data, like Amazon, Facebook and Google, and that gives great cause for concern. I am just wondering if that type of technology covers your vision, at all, for the future.

Brigadier General Robert Spalding: Unfortunately not. The only way that you do it is really by encrypting the data, and I would argue that you



have to get to a post-quantum encryption. On the blockchain technologies themselves, you have proof of work and proof of stake. For proof of work you've got a quantum computing vulnerability that you hack the hash once we get to a powerful enough quantum computer. On proof of stake, it really depends on the security of the platform that you are running that blockchain on. If you are on an insecure platform like we have today, you really cannot verify the security of that implementation. Those are two great applications that, again, require to be laid over a secure encrypted network.

Q105 **Martin Docherty-Hughes:** Thank you. I don't know if Mike wants to say anything on that.

Mike Rogers: Think about how we got here. Remember tech companies like Google and Facebook and others are really very tech-savvy advertising companies. Their revenue is based on advertising, and that advertising is based on you. I always say that if you are getting something for free, you are the product. That is exactly what they did. They gave it to you for free and said, "By the way, the product is you. I'm going to track everything you do and watch everything you do, and then I'm going to market back to you things that I think you want to buy, to make it more efficient." That's the model we are in, and until we change how that works we are going to be in this for a while. Candidly, most people are accepting of that: I am willing to do Facebook knowing that they are going to send me ads, because I get it for free and I like some of the ads. Until we figure out a way—and I happen to agree with the General: we are never really going to get encryption at a state until after encryption at quantum-level computing; then it's much, much more difficult to find and get, so that only nation states will get it, versus criminal enterprises—we are going to be in this transition.

The argument about how you protect that data—it is one of my arguments about why we would allow Huawei in liberal democracies around the world, knowing that they have diverted data to China before and that, when they get their hands on that data, they use it for purposes that are probably adversarial to our interests, including the citizens' data. You mentioned information operations. You had seen what happened in 2016 in the US: limited information operations, which were pretty aggressive. Now we see the Chinese doing the same thing. Their ability to manipulate data, to get you to think one thing or another, is on the rise. We know they want to interfere in elections; we know they want to put out their part of the story. This is something we ought to focus on and worry about, because it is coming. We already see what is happening now, and it's coming.

Chair: We're up against the parliamentary clock, but we have two very quick questions. We will ask both Richard Drax and Bob Seely to give their questions, and maybe you could just wrap them together. Richard, do you want to go first?

Q106 **Richard Drax:** Gentlemen, this is the question that I, as an ex-soldier, have debated more in my private time than any other question. Have our militaries become too reliant on data and high-tech systems? For



HOUSE OF COMMONS

example, I understand there is a pulse bomb; if it takes out all the technology, all our ships and modern technology will be absolutely useless, and we will be back to the pop gun—the 6 inch, 10 inch or whatever it may be. Have we become too reliant on this for a future war, and do we risk an enemy with the sufficient kit putting us back into the stone age?

Q107 **Bob Seely:** May I make a declaration? Last year, I co-authored with Brigadier General Spalding and others a report entitled, “Defending our Data: Huawei, 5G and the Five Eyes”, which was published by the Henry Jackson Society. My question is to the Brigadier, and indeed to Mike Rogers. My apologies: I have been out voting, so I hope we have not asked this already. How can smaller software firms effectively engage in building up our new advanced 5G networks, or do you have to have scale? Do you have to be a tech “giant” to be an effective player in this market?

Brigadier General Robert Spalding: I have lived through this in the US air force. We started back in the early 2000s to shut off our GPS and shut off our radios. The challenge that that brings to the military forces is that it gets us used to fighting in the stone age, and then we forget about the fact that, if that stuff gets shut off, we’ve got chaos in the streets. If we shut off GPS, the grid and the cell networks, there is no way we are going to be fighting abroad, because we will have to bring peace to the streets. We have lost focus on how important these technologies have become to our societies, just to keep them functioning as civil societies. So no, I think that is actually harmful; it really prevents us from building EMP-hardened, resilient, military-grade IT systems that actually take a licking and keep on ticking. That is what we need for our society. If you shut off the internet or shut off the power in a major city, you’ve got chaos in just a few hours. This is something that we know and, quite frankly, it is irresponsible of the military to think in terms of, “Well, we’re just going to shut off everything,” because it is not thinking about the implications of that if it happens in our own society.

On the other question, the big problem that we have for scale is, again, cost of radios. We need to get the cost of the radios down, so that we can really deploy. In terms of the software though, yes, it is very easy to scale as long as you have an antenna and a radio. If you don’t have an antenna and a radio, you cannot scale like a typical software company in 5G.

Mike Rogers: Certainly, our adversaries knew this. Looking at the Chinese defence posture over the last 15 to 20 years, they realised the advantages we had in smart soldiers, smart bombs, smart airplanes and smart aircraft—the whole nine yards. They adjusted to that, and they would try to develop a defence plan and an offensive plan that would go after our ability to have smart airplanes, smart bombs and smart soldiers. Candidly, they were a little ahead of us on this. We thought we couldn’t get caught up; they were aggressive.

To make that point come home, the United States Naval Academy, starting in 2017—they had not done this for, I think, over 20 years—



HOUSE OF COMMONS

required that every new commissioned officer in the navy who came out of the Naval Academy in 2017 and subsequent classes had to understand a very important piece of technology to compete. That was the sextant, developed in 1728. They had gotten away from it, so they decided they had better get back to it, just in case those GPS systems weren't working. I think that brought the point home to the military: "Okay, we've got some issues. We've got some problems. We have to get around it."

To the General's point, this is why the Russians tried to get into our electric grid; it was announced by the Administration that they had found Chinese intelligence efforts to get into our electric grid—and when I say ours in the US, trust me, they are trying to get into yours as well. That creates a problem because they know if they turn off the lights, they get chaos in the streets. They get such level disruption. You couldn't get gas, you couldn't pump gas, you couldn't get cash out of the ATM, you couldn't even do a credit card transaction online—all done. Imagine the chaos that that would create. We have to start looking at both a military and a civilian protection of these networks.

If you go down to the basic point, do you really want to take the risk? Do you want to roll the dice that Huawei is going to be a good player and that China is going to co-operate when you need them to co-operate the most? I think history has shown us that that is not the case. I would be extra careful on that, and then look at how we build out systems that are secure and ensure that we secure every piece of data.

On the small company thing, listen: I am an entrepreneur and have invested in a couple of small companies that do exactly this. It is hard; it is not easy. You lose a lot of sleep, and sometimes you lose some money—but at the end of the day, the innovation that is generated in there to try to solve these really hard problems is exciting to be a part of. I think that spirit is alive and well in the United States.

DOD is reaching out and trying to find ways to talk to these companies—innovative ways. Actually, the Air Force has a really good programme, where they can give a contract at the end of the day. You can come out to the showcase and if they like it, they can give you development money at the end of the day, which is nearly impossible in the US system. Why? They are trying to find these small companies and these small entrepreneurs. Sometimes, guess what? Big tech isn't going to solve the problem. It is going to be the small innovative tech leaders that come out and go, "We have a better way. We've got a better mousetrap here, and we just need somebody to see it."

We are in that time right now. That is what we are doing right now in the United States. To me it is a very exciting time to be here. It is an exciting time to be talking about the 5G problem, because it can be such a massive opportunity for the betterment of all those liberal democracies, as has been mentioned.

Q108 **Chair:** Thank you for that. I have just read a fascinating book by Jim Scuitto called "The Shadow War", which you might be familiar with. It



HOUSE OF COMMONS

talks about the changing character of conflict—where we are heading with this global clash of ideology. It won't be on the conventional field; it will all be very much in the digital space that we are talking about. Do you concur?

Brigadier General Robert Spalding: Absolutely. My book, "Stealth War" explains exactly how that happens. It is based on my last five or six years in service, where I was focused on US-China competition, and it shows how they have moved warfare out of the traditional battlefield into the area of globalisation and the internet, and turned all of our once strengths into vulnerabilities by undermining each and every one of them. When you understand how that truly works, you realise that we as a community of free nations have really lost sight of what is important when it comes to protecting our democracies.

Chair: Thank you very much indeed for helping us out today with our inquiry. It has been really illuminating. General, I appreciate your time. Mike Rogers, I understand it is your birthday today—is that correct? You spoke earlier about having a pint or two.

Mike Rogers: It sure is, and I wanted to spend it with all of you.

Brigadier General Robert Spalding: Happy birthday.

Chair: We are very honoured. I want to pass on best wishes from Sir Nicholas Soames, formerly of this place.

Mike Rogers: He is a good friend, and always good for a good quote at dinner.

Chair: Absolutely right. We miss him dearly here.

I thank you both, and I extend my thanks again to Senator Tom Cotton. It has been an instructive and illuminating afternoon. Thank you again to my colleagues on the Committee. We are very grateful for your time.