Steptoe

Episode 235: It's a Bird, It's a Plane, It's...Doug?

Stewart Baker: [00:00:04] Welcome Episode 235 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thank you for joining us. We're lawyers talking technology, security, privacy, and government. Today I'm joined by our guest for the interview, Doug, no last name allowed, the general counsel of the – or the chief legal officer of – GCHQ, which is the United Kingdom's version of NSA, plus a whole bunch of other stuff as we'll hear. Also joined today by Nick Weaver, who is a senior researcher at the International Computer Science Institute in Berkeley and a lecturer at UC Berkeley. Matt Heiman is a visiting scholar at the National Security Institute, formerly with the National Security Division of DOJ. And I'm Stewart Baker, formerly with NSA and DHS and today's host. Why don't we jump right into the story that won't die? Nick, I can't believe that we're going to end up talking about the Supermicro alleged hardware hack by the Chinese again for another week and we still don't know if it's true.

Nick Weaver: [00:01:14] Yeah, and the problem is the *Bloomberg* has doubled down without any independent evidence. So the new *Bloomberg* piece is describing a different attack, which unlike the original attack is not plausible in my mind because it's describing Trojan Ethernet jacks. And Ethernet jacks need a lot of processing power if you want to do something in the jack, and the jacks are unpowered. So although the original attack proposed was not only frighteningly plausible but I could develop the infrastructure for it for a million bucks (hint hint, NSA), but the new one, it just doesn't make sense. And although it has a named person behind it, there is no evidence provided. The companies all deny it. And at this point between all the denials, including like Rob Joyce of the NSA with his very strong denial –

Stewart Baker: [00:02:16] And the director of the FBI and DHS. All of them. One variant or another of "Don't believe everything you read" or "we can't confirm that," right?

Nick Weaver: [00:02:27] No. Rob Joyce's was even more: we have no bleeping clue what this is, and if you guys have anything, please tell us. We want to know about it.

Stewart Baker: [00:02:37] Yes, you're right.

Nick Weaver: [00:02:37] That's a strong denial.

Stewart Baker: [00:02:38] He said, "I see a lot of intelligence, and I don't think I've seen this." So yeah.

Nick Weaver: [00:02:45] Yeah.

Stewart Baker: [00:02:45] It's pretty remarkable because Bloomberg has not backed off at all. They say they've got the sources. And you know you just have to either trust them or trust all the people who are denying it. I have to say there's a legal issue here. The companies that are denying this, if they are actually lying, have a real SEC problem and FTC problem as well.

Nick Weaver: [00:03:15] Yeah. And at this point I really think there'll be a tendency to call this a false alarm. I think we should call it an alarm clock. We need to get much more serious about designing things. So, for example, the iPhone actually does it right. You could not use this attack against the iPhone because the iPhone is designed not to even trust Foxconn.

Stewart Baker: [00:03:38] Not even to trust its own motherboard then.

Nick Weaver: [00:03:41] Correct. It doesn't even trust its own motherboard. The only thing the brains in the CPU trust are stuff signed by Apple, so you'd actually have to sabotage the CPU itself. You could not use the technique described in the *Bloomberg* article.

Stewart Baker: [00:03:57] So one of the things that influences me here is that these guys have come up with stories in the past that nobody else has been able to confirm. There was the great story that I believed for years that the Russians had been spotted walking along a Turkish pipeline by an infrared camera that was the only remaining way of watching the pipeline, and no one's confirmed that one. And the suggestion that NSA was using the Heartbleed bug for years before it was discovered has been pretty thoroughly denied by NSA, and nobody has come back to say that wasn't true. There's a track record here of very controversial stories that don't have much in the way of later validation.

Nick Weaver: [00:04:51] Yeah, and the other thing is some reporters notably Brian Krebs. Brian Krebs came forward and said he had heard the same rumors about Supermicro but was unable to get confirmation.

Stewart Baker: [00:05:05] I'm going to suggest that what we need for the new world of journalism is not a Pulitzer but a Bull-itzer. This is just bull. And once we discover that a story is bull, we should award Bull-itzers to the journalists who've produced them. You know there's a long history of this. There was that guy in the *New York Times*, Walter Durante, who wrote a whole series of stories in the '30s covering up the Ukraine famines and the use of famine as a political weapon because he thought you know the Soviets at bottom had the good of humanity at heart and what's a few Ukrainians if you're trying to achieve a global transformation. So you know journalists do sometimes let their ideologies get in the way of telling the truth. And it is possible that that happened here.

Nick Weaver: [00:06:05] Yeah. Or what's more likely is some really bad game of telephone that the problem is the reporters in question, their sources do not seem to be the engineers.

Stewart Baker: [00:06:21] So there's somebody who heard this and didn't hear the final outcome or heard a version of this and is attaching things they heard to the wrong story.

Nick Weaver: [00:06:35] Right. So, for example, Apple did ditch Supermicro three years ago, but the reporting at the time, which I think may be confirmed, is that Supermicro screwed up and released a sabotaged BIOS [Basic Input/Output System], not a sabotaged motherboard, that was downloaded. Apple caught it and goes basically, "These guys are too incompetent to buy it from again."

Stewart Baker: [00:07:03] Yeah. So there's probably something here, and it sounds as though it may be a good deal smaller this time around. But I have to say it's only a matter of time before it turns out to be true, right?

Nick Weaver: [00:07:14] Especially because if you're China, you look at it: if you've done the time, you might as well do the crime.

Stewart Baker: [00:07:22] [Laughter] Alright. Speaking of China, the Trump Administration continues to draw a bead on China. The CFIUS process – Michael Beaver has reminded me not to assume that everybody knows what CFIUS is. CFIUS is – C-F-I-U-S – the Committee on Foreign Investment in the United States. It's been around for 40 or 50 years, and it decides whether we're going to let foreigners invest in US companies, and it's gone through several cycles of fear of foreign investment, the latest being fear of Chinese investment. And that is very real and very substantial, and we are in the process of reordering all of our legal institutions around a fear of a challenge by China. CFIUS has been rewritten by the Congress, and it is now up to the Treasury Department to implement rules, some of which are quite complicated and could add enormously to the burden of the Treasury Department because of the large number of people who will have to say, "Oh, yeah, I made that investment. Oh, yeah, I made that investment. Is it okay?" And Treasury has risen sort of to the challenge with a pilot program that they released this week. Matt, what did they actually say they were going to do?

Matthew Heiman: [00:08:52] Well, they said that they were going to have some interim rules until they have their permanent rules, and the pilot program is part of those interim

rules. And it covers about 27 industries which, depending on how elastic you view those categories, covers nearly everything of importance.

Stewart Baker: [00:09:10] Staggering. This is the thing that surprised me. I expected them to use this pilot program. I thought it was actually a clever thing on the part of Congress to say, "Do a pilot and see how many filings you get." But the list of industries that they wanted covered was staggering.

Matthew Heiman: [00:09:28] It covers seemingly everything, except plastic wrap. I mean it's a wide range, and it's all the industries that Chinese actors would want to invest in – or for that matter, any other foreign investor. And the other piece of it that I thought was interesting was this – you know and clearly the new CFIUS legislation is moving away from the notion of foreign control to just any sort of foreign presence. So it talks about you must report if the foreign investor has access to non-public information, which would be seemingly any investor in any entity would have some non-public information, or you have the power to nominate a board member. So I think the other thing, just it's useful for listeners to keep in mind, is while a lot of the energy around CFIUS reform is clearly focused on China, if you're doing a deal and you've got a French party that's interested, you've got an Irish party, or wherever they are in the world that's looking at buying US technology, it may scoop them into that deal. So yes, China certainly is the focus, but the new CFIUS reform's gonna apply across the board.

Stewart Baker: [00:10:37] The pilot program though is focused on China.

Matthew Heiman: [00:10:38] It's focused on China. But the point I'm making is that the new beefier CFIUS applies to all players.

Stewart Baker: [00:10:45] Yes, and in the long run it will. But I'm guessing that what Treasury is going to do is see just how much stuff comes out of the woodwork by focusing on China, which you know since that's their worry makes sense for them to do it. And then once they see how many deals come forward, they will titrate exactly what they're going to require for everybody.

Matthew Heiman: [00:11:09] I think that's right. And you could assume that there are further rules that might give different actors different planes of scrutiny. So one could imagine that China and Russia would be on one level and Switzerland might be on a different level.

Stewart Baker: [00:11:23] Right. And I will also say the good news for Treasury is that even before they put out this rule, I thought that Chinese investment was already waning pretty substantially as the Chinese government issues guidance that says, "Yeah, maybe it's not worth doing." And that means that Treasury may not get as many deals as they were afraid of.

Matthew Heiman: [00:11:52] I think that's right, particularly given that the push by leadership in China to domesticate a lot of these technologies. Rather than going out to the US to buy them, they want to create them at home because that gives them maximum control.

Stewart Baker: [00:12:04] So when they can't create them at home, however, the Justice Department has a message: don't create them at home by stealing them from American companies. Nick, those of us who said, "You know indictments are okay, but they don't really have an impact." We reckoned without the reach of the US government, which has actually snatched a guy off the streets of Belgium who was spying for China and pulled him into the United States to prosecute.

Nick Weaver: [00:12:33] And good on the Justice Department. I think this is the distinction between the human side and the SIGINT [signals intelligence] computer break-in side of industrial espionage. So this guy was targeting GE engines and others, but it was a largely human-driven scheme. Invite potential contacts to give a visiting lecture in China and scope them out then. And so that requires a lot of local presence in both the US and Europe in order to do this recruitment. And so as a consequence, being within range of US law enforcement, he is going to be a guest of the federal government for a good long time. I do like the computer hacking indictments too though

because they allow the US government to put its cards on the table and actually attribute some of these things, like the North Korea one I found really insightful as cards on the table evidence that North Korea is hacking for profit as a money source.

Stewart Baker: [00:13:49] Yeah. I agree with you that there is value in laying that out, going through the exercise of saying what can we declassify, and I'm sure there's a great fight under the covers about what goes into those indictments, but there is value in doing that. I noticed that one of the stories over the weekend was about Intrusion Truth from the *Wall Street Journal*. And I can't help thinking that Bellingcat and Intrusion Truth and some of these other quasi-anonymous sources about Russian and Chinese cyberattacks might not be benefiting from some of the intelligence as well that's being released in a fashion that doesn't attribute it back to the United States. Some of the stuff that's coming out in Intrusion Truth is also very focused and would require that you do something more than just look at the source code of the malware.

Nick Weaver: [00:14:54] I haven't looked at them as much as Bellingcat. Bellingcat at least is doing a huge amount that showed their work.

Stewart Baker: [00:15:01] Yeah. Well, let me put it this way. If I were in government, I'd be saying, "Why the hell don't we have some place where we can anonymously embarrass the Russians and the Chinese and out their tools and their people?"

Nick Weaver: [00:15:21] After all, they have WikiLeaks!

Stewart Baker: [00:15:23] Yeah, exactly! Exactly! And DCLeaks. And WikiLeaks really hurt the US intelligence community. So the idea of giving it back is going to have an enormous appeal. So maybe it's not Intrusion Truth. Maybe it's not Bellingcat. But I got to believe that somebody has found a way to channel or funnel information that they think would be embarrassing to the attackers on the other side to the public sphere. Okay. So there's one place that doesn't want to choose sides in this growing battle between authoritarian and non-authoritarian governments, and that turns out to be Silicon Valley. Google is saying, "Yeah, you know we're just not going to bid on those AI

contracts that the Pentagon has asked people to bid on because it's inconsistent with our values." You kind of wonder how they're also developing a search engine for China consistent with their values, but they're getting some flak locally from their own employees about that. But it's very disappointing to see their employees unable to draw a distinction between the Chinese government and the US government.

Nick Weaver: [00:16:46] I think actually their employees are drawing a parallel of negative to both that the problem is the greatest trick the devil ever did was convince the world he didn't exist. Number two was convincing people and employees that "don't be evil" meant something. And so Google ended up hiring a lot of people with a very strong idealistic streak. And when the rubber hits the road, it tends to produce conflicts. Even though, let's face it, Google is a spy agency that makes the NSA seem embarrassed by the amount of data they collect.

Stewart Baker: [00:17:28] It's true. They don't have near the storage or frankly, probably, the sophisticated algorithms. So Matthew, I guess I should say, is this just a bluster because they probably weren't going to get the contract anyway?

Matthew Heiman: [00:17:45] It certainly seems that way. I mean when you hear the phrase "burying the lede" and you read the news clipping that says, "Well, it doesn't jive with our AI values, and by the way portions of a contract are out of scope with our current certifications."

Stewart Baker: [00:18:00] [Laughter]

Matthew Heiman: [00:18:01] It certainly makes me think –

Stewart Baker: [00:18:03] So they had not even qualified for this contract.

Matthew Heiman: [00:18:05] No, no.

Stewart Baker: [00:18:05] So this is grandstanding after a fashion.

Matthew Heiman: [00:18:08] Well, it's making the most out of a loss, right? So we know we can't win this, so let's put some stilts up and sort of proclaim our values along the way.

Stewart Baker: [00:18:19] But you know I wish their values did not assume that helping the Pentagon was a bad thing. There'll be a time when helping the Pentagon will seem essential, is my guess, sometime in the next 15 years.

Matthew Heiman: [00:18:36] Yeah. Well it's consistent with most of what Alphabet does, which is what they think is best for the bottom line, and right now that's helping China, not helping the US. But that, as you say, may well change soon.

Stewart Baker: [00:18:49] Alright. Well, they're struggling to figure out a way to help the EU. Google has appealed the massive fine that was imposed on them. Did we learn anything from the appeal. Matthew?

Matthew Heiman: [00:19:06] Not especially, other than I think it's just a useful reminder for people that think antitrust is a panacea for what they perceive as market ills. I would suggest that we'll probably go through a similar experience as we did with Microsoft 15 years ago or so, which is by the time we get to the end of the story, the technology and the market dynamics will change so radically it's virtually meaningless to the marketplace.

Stewart Baker: [00:19:28] This was a shopping display bias – not a shocking one, but shopping. You know I never use Google to shop for stuff. They could have all the display bias in the world, and it wouldn't affect me. And I suspect that's true for most people. So this is a $5 billion fine for doing something that didn't work.

Matthew Heiman: [00:19:49] Yeah. It's related to that as well as the notion that Google was paying manufacturers to favor Chrome and search over other Android platforms,

but again I think by the time this is all resolved years from now, it'll be virtually meaningless because the players and the platforms will have changed.

Stewart Baker: [00:20:07] So but what does happen is companies go through a period of believing that they don't need governments and they can just do what they want and governments will suck it up and then they have a conflict, and then you know the EU or somebody just comes down on them like a ton of bricks and they are permanently maimed. IBM was permanently maimed by the US antitrust case. Microsoft, which wanted to be the anti-IBM – "we will never be maimed by the government, we will by God just soldier on" – they're maimed and have changed their tune. And I suspect that for good or ill Google and Facebook are now in the sights of the ton of bricks that the EU has prepared.

Matthew Heiman: [00:20:56] I think that's right. I think you could also look at it as when governments do this, the size of the buildings for the respective company in that capital grow immensely.

Stewart Baker: [00:21:06] Yes!

Matthew Heiman: [00:21:06] The number of lobbyists grows immensely. So maybe in a roundabout way, the EU views this as an employment opportunity for their citizens to go work for Google, who'll now have a much bigger presence in Brussels.

Stewart Baker: [00:21:20] So if you wondered why you listen, if you were a law student, to the podcast, it's because we give you career advice like that: you should be preparing your résumé so that you can send it into the European Commission or maybe the Justice Department's antitrust division because understanding technology will give you a career for the next 15 or 20 years. Alright. So DOD cybersecurity – this is relevant to the question of hardware hacks. Our weapons systems, GAO says, are not actually all that good. And the White House says that's because our entire defense industrial base is on life support. Nick, did you take a look at those two reports? And how worried should we be?

Nick Weaver: [00:22:14] I skimmed both of them. The GAO one is very worrisome because the problem is I think a large outgrowth of how the DOD has designed their networks. You have system low side which is assumed to be a cesspool, but system high side everybody is trusted. But that means that if an adversary can get in system high in one spot, you can do all sorts of things. The [White House] industrial base report I didn't find as impressive because, let's face it, we could not build fighter jets for three years and it wouldn't be a problem. What we really need to focus on is what systems do we trust in our manufacturing because a problem of trust in manufacture cannot be corrected. A problem of supply just disrupts future purchasing. And like, as I said, some of the things don't read right, like there was a complaint about the US manufacturing base for rigid-flex circuit boards and many-layered boards and high-precision assembly die-ing, and frankly that is a pile of bovine excrement. Why do I know? Because I built my own boards by contracting out to a Silicon Valley [company] that will do 20, 30, 40-layer rigid-flex boards with ITAR [International Traffic in Arms Regulations] compliance. So I know that part of the industrial base there's at least some in the US, and it's not as dire a picture as that report suggested.

Stewart Baker: [00:23:58] Okay. Well that's good to hear. It is interesting to see how the Trump Administration and the president's unhappiness with China – well, you know this is a lesson in bureaucratic behavior. The president came in saying we should be nicer to Russia, we should be meaner to NATO and to the European Union, and meaner to China, and the bureaucracy has picked that up and said, "Yeah, not so much on Russia, and we can be a little meaner to the EU and a little bit meaner to NATO. But we'll tell them it's because they're not spending enough." And then China: "Yes, sir. Very much so, sir." And they've gone out and overachieved to the point where everybody in the US government is thinking of ways to strengthen the US military and quasi-military posture against China because they were worried about that even under Obama. And so they're happy to get guidance that accords with their preexisting concerns. I think that means that Trump's effect on our relationship with China is permanent and transformative. And this is all part of worrying about a future in which we have a peer – or it's a near-peer in that in that we are almost as big as they are – for the

future, and the US is struggling to figure out how do we build a strong geopolitical situation where we can't count on our economy to power us past the competition. So bad news. Speaking of picking sides in the great battle: Vietnam has said to Silicon Valley, "You know we sort of like the idea of localization of data as well for national security reasons, etc.," and Silicon Valley is saying, "But, but, but, but Ira Magaziner! And you know John Perry Barlow!" And Vietnam is saying, "Yeah, never mind." Matthew?

Matthew Heiman: [00:26:08] I think it's another link in the chain. I mean so this is what Russia did a few years ago. You know Vietnam's doing it. I think everyone's going to do it at some point. There's no downside for a national government to not do it.

Stewart Baker: [00:26:20] So you know one of our national strategy statements on cyber coming out of the Trump Administration was all the stuff that John Perry Barlow lyrics could have produced, right? The Internet ought to be open and free, and there shouldn't be national boundaries. You kind of wonder when they're going to give that up. You would have thought that would have been something that the Trump Administration would have chucked overboard.

Matthew Heiman: [00:26:47] Yeah, well they can cling to this dream, or they can get with reality because I think that's the march –

Stewart Baker: [00:26:53] So you know clinging to the dream has a cost because they end up saying to policymakers, "Well, you can't do that because it's inconsistent with what we've been telling the world that you ought to have a global open Internet," which means that when people say, "You know that data shouldn't leave the country," the State Department and others say, "Oh, you can't have a policy like that because it's inconsistent with our international posture," which everybody else is ignoring.

Matthew Heiman: [00:27:21] Yeah, I think that's true. But I think you could also wind up with a situation where you have different realms of kind of these walled Internet states, so I think you could have localized data in places like Vietnam and China and Russia,

and you could have localized data between the US and the EU within the confines where data flows within those boundaries. But I think there are going to be pockets of more authoritarian regimes that say, "We want all the data and all the servers here."

Stewart Baker: [00:27:47] Yeah, look, my thought is especially for the Russians, there may come a time when we say, "You know you want to have your own Internet? Let us help you with that. Ah! Did we just drag up all of your cables to the outside world? Ah! What a shame!" And that may be a more effective sanction than whining about the openness of the Internet. Okay. That concludes our News Roundup, and I'm on to the interview which I actually recorded on Friday when I was – we had Doug in the studio and me trying to do this from Italy, and I'm afraid we got an Italian Internet connection, so I hope the audio is good. But let's turn to Doug.

Stewart Baker: [00:28:39] This is the first interview I've done with someone whose last name is more or less classified, can't be used. It is the chief legal officer and I think international policy expert at GCHQ, which is the equivalent of NSA, in the United Kingdom. "Doug," as he's asked us to call him, is the equivalent of general counsel of the National Security Agency, more or less the job I had. Doug, my first question I guess for you is: if you have to have a pseudonym, shouldn't you have picked something sexier than "Doug"?

Doug: [00:29:31] Well, the problem is if you come late to the party, you've got to take what's left on the table. And sadly "Saul Goodman" had been taken by someone else, so I'll have to live with "Doug" for the time being. Thank you for that though, Stewart.

Stewart Baker: [00:29:45] I'm glad that you did it. It's actually not a bad pseudonym because no one would guess that it was a pseudonym. So Doug's last name is not to be used, and we've agreed to that. But he is glad to talk to us about what it's like to be the chief lawyer for GCHQ. And I'd like to kind of jump into that because when I was at NSA as the general counsel, we envied the British, their oversight, which was restrained more or less singular as opposed to multiple and often could be accomplished in an afternoon, including the drinks. And that has changed is my sense that there is a good

deal more oversight. It's much more exacting than the oversight position that we're used to in the UK. And I wondered, Doug, if you could just give us a sense of how oversight for signals intelligence and intercepts has evolved over the last, say, 10 years?

Doug: [00:31:06] Sure. I'll do my best, and I have to say I wouldn't necessarily agree with every characterization of the regime, at least in my experience and the experience of my team members. For some time we've had a rigorous oversight regime, and it's come in a few different forms. There is the Judicial Commissioners now, as you rightly say, has sort of consolidated into one office, the Investigatory Powers Commissioner. That was done in the Investigatory Powers Act of 2016, which is sordidly described as our license to operate for the Internet Age. On top of the Investigatory Powers Commissioner, who has 15 judicial commissioners working for him and 50 inspectors and staff or thereabouts, we have the Investigatory Powers Tribunal, a senior court in our system in the UK. We have the Intelligence and Security Committee, and we have the other courts which have jurisdiction over several of our issues, including the European Court of Human Rights in Strasbourg, the Court of Justice of the European Union in Luxembourg, and even they're the only permanent member of the Security Council who has adopted mandatory jurisdiction of the International Court of Justice. So you have a menu. You have a number of different options for oversight. I can tell you as someone who is dealing with the regime as it is now, it is rigorous, it is independent, and the caliber of personnel, judges, and other staff members who are coming into the space is impressive. And it's quite an experience to be overseen by them. I can say that much.

Stewart Baker: [00:32:46] I bet. I've certainly gotten the sense that there has been a great deal of change in the oversight regime. And I certainly don't envy you having gone through oversight. I used to say that there were at least six different offices where the head of the office his career would he made if he could catch the National Security Agency breaking the rules. And my guess is that you have at least two or three such offices yourself.

Doug: [00:33:22] Yeah. I mean we have a number of internal sort of parts to the system whose job it is to help the mission comply with the applicable laws and policies that we put in place to get that balance right between protecting privacy and safeguarding security, and you know people are going to have different views about this. But for us the way the weighing of those two key principles has been done by our Parliament and this Investigatory Powers Act and what we're trying to do internally – or what we are doing internally – is putting in place the culture, the systems, the training, and the engagement with our oversight so that we can get it right because everyone I've come across at GCHQ wants to comply, wants to follow the rules. They want to follow the law, but they also want the legitimacy that that democratic oversight comes with.

Stewart Baker: [00:34:20] So one of the things that at least GCHQ has had to worry about – I think there's less concern of the National Security Agency – is what the law of war says or what restrictions the law of war might impose on the kinds of activities that both GCHQ and NSA have been engaged in, principally cyber actions whether for espionage or for other purposes. How much does the law of war enter into the job that you have to do, Doug?

Doug: [00:35:04] So it's certainly part of the picture, and it might be helpful just to put it in a bit of context because one thing that hopefully won't surprise people but it sometimes does is that we comply with all the applicable law whether it be UK law, the European legal regimes that may apply (the European Court of Human Rights, EU law where it bites), but also international law. That's sort of written into the code of the British government, and that applies to GCHQ and the other intelligence agencies as it does to any other part of government. What that means in practice is we both look at, as I mentioned before, the kind of privacy angle, the intrusions into privacy, the human rights implications of what we do if you like at the front end, but we're also looking at the backend, the uses to which our material might be put. So GCHQ has got three basic missions: to provide intelligence, to bring about effects, and to safeguard cybersecurity. We do that for the purposes of national security, economic well-being, and the prevention and detection of serious crime. That might come into – to give it life – that might sort of be best exemplified by our work supporting UK counterterrorism efforts, to

help bring down rings of child sex offenders online, to help find, call out, and stop hackers whether they be criminals or actors of foreign states. But it also involves supporting the military which is a role which goes right back to our founding practices and our history, and our centenary is coming up next year where we're going to be both looking back to successful incidents in our history such as Bletchley Park where with others – Americans, Poles, and a plethora of international experts – we helped crack the Enigma codes and the work of today that we're doing to support the military. And that might be where a whole range of international legal rules come into play. Then-British Attorney General Jeremy Wright made a speech on this. And part of that is the international humanitarian law, the law of war, but it's not the full picture. It's cited in the sort of wider framework of international law. And I think – and I'll stop after this point – I think you can sort of overplay the militarization of cyberspace in some situations. There's a lot of cyber activity and intrusion that happens below the level of an armed conflict. And I think one of the key challenges is: how do we, as state-responsible actors who want a rules-based international order, how do we address those incidents below the level of war in that sort of gray area? And that's one of the challenges where we're most focused on in GCHQ.

Stewart Baker: [00:38:11] NSA of course has famously – or the military has created the Cyber Command, which is overseen by the head of the NSA, but there's a lot of effort to separate the two quite completely and then put NSA in a position where it is supporting Cyber Command. And that means that the legal advisers for Cyber Commander are different from the general counsel at NSA. How does that compare to the organization in the UK? When you support military are you operational, or is there somebody else who would consider themselves the equivalent of Cyber Command?

Doug: [00:38:56] So we don't have a Cyber Command as such, but what we do is sort of – there's two parts to this and they both overlap and interrelate. The first part is, as I said, one of GCHQ's fundamental roles is military support. And so that's part of our core mission, and it's something we do whenever it’s required. That might be providing a range of functions and support facilities to the military. And when we do that we're looking to integrate with them and support them. On the other side, we have military

working for us. That's built into our sort of founding statute in the Intelligence Services Act of 1994, and when the military are working with and assisting GCHQ they are actually considered for the purposes of our capabilities as part of GCHQ. They retain their own rank structure, discipline, and so on, but they are considered part of GCHQ and therefore the level of integration we have gives them access to our capabilities. And in doing so they have to follow our rules and are subject to the same training, compliance, and cultural requirements that I was talking about before. I think given the challenges in this space further and deeper integration will be needed in future, and I'm sure I would predict sort of news on this front before too long.

Stewart Baker: [00:40:21] So one of the things that the US has been struggling with and other countries have been struggling with and your attorney general laid out the UK view pretty clearly is: what are the international rules that govern operations in cyberspace? To what extent and how does the traditional law of armed conflict apply to the operations in cyberspace? I tend to be skeptical of efforts to construct even modest sets of rules that translate to the law of armed conflict directly. My sense is the UK has been much more focused on establishing that what it is doing is consistent with the law of armed conflict and that there are rules. Do you see a differentiation among countries, especially Western countries, in terms of their enthusiasm for laying out the details of the armed conflict rules that they think apply to them in cyberspace?

Doug: [00:41:37] I think there's more we agree on than we disagree. I think that this is still an emerging area. So there's plenty of room for further fruitful discussion. I mean the UK, like other Western countries that share our values, wants to be open and clear about the rules that we are bound by. We think – or least we hope – that in doing so we're not only demonstrating our commitment to that rules-based international order that's for us a cornerstone of our foreign policy, but we also hope to shape the understanding and the development of the rules and that's by populating the debate with as much state practice and views about that *opinio juris* as we can. And to me the question is not anymore whether international law applies in this area. It's how it applies and whether it's enough. And that's something our attorney general said earlier this year.

Stewart Baker: [00:42:35] Thinking about that, obviously at the end of the day international law is the practice of nations when they think they are doing something that they must do. And I noticed that the attorney general quite rightly said there are rules about – international humanitarian rules with respect to the law of war – protecting civilians, making sure that your actions are proportionate. And yet if I were asked is it proportionate when you have a beef with somebody internationally to come up with a piece of malware that wrecks networks far from the field of conflict – and it doesn't matter whether you're talking about North Korea or Russia. They've clearly unleashed tools on the world that had effects well outside the borders of the state they seem to be interested in influencing, and there wasn't any sign that they spent ten minutes thinking, "Gee, what would happen if this particular tool escaped the Ukraine or spread around the world and bricked a bunch of computers in the National Health Service or where have you?" I guess my question is: how does it feel to be announcing rules of proportionate response and proportionate activity in a context where it isn't at all clear that the people that are our most active adversaries recognize those limitations?

Doug: [00:44:23] I can see the challenge entirely. I mean for me there's two parts to the response. The first is that the way international law applies in this area – at least as we see it, and as we've set out publicly and hope to develop further in public and in future, at least I would hope so – you can actually respond effectively and robustly but do so responsibly and lawfully. And we're trying to make the case for that. We're trying to demonstrate that. We're following up with practical examples of what types of behavior should be considered in which category and what's beyond the pale basically. The second part of it is – you say why should we bother with this if other countries, our potential adversaries aren't doing it – and to me that's about what kind of countries we want to be, and it's about the integrity and security of a new domain of life, the cyber world which impacts everything that we're doing, impacts the way we're carrying out this interview. And for me it's just not – law to one side – it wouldn't be a responsible or even sensible option for the countries that uphold the international order to be acting indiscriminately or disproportionately. It's not in our interest to do so. And I come back to

the first point. The law sets sensible parameters around this but allows you to act and acts necessarily, proportionally, but vigorously.

Stewart Baker: [00:45:55] Yes I see the point. We can certainly act vigorously. Whether acting vigorously is sufficient to deter the kinds of activities that we've seen from adversaries is a different question. There is not much sign that at least the Russians are reducing their activity or even showing much sign that they're afraid of getting caught. The most remarkable development of the last five years is that the Russians have gone from being very stealthy and very effective at hiding themselves to apparently not giving a damn whether they get caught, even with their Uber receipts leaving from GRU headquarters to the airport when they're carrying out missions. And so at the end of the day, if we can't deter with the tools that we think we have, then it's not clear we can enforce the rules that we think exist.

Doug: [00:47:01] I see the point. I mean my answer would be that we are deterring, that we are by calling out Russian actions. And we saw the foreign secretary of the UK spent recently calling out the activities of the GRU and attributing those activities to them and to the Russian state. And that attribution was backed up by I think over 20 other countries. So by calling out this kind of behavior, by acting in tandem whether it be bilaterally through multilateral institutions such as the OPCW [Organisation for the Prohibition of Chemical Weapons] in The Hague, I think we are as a group of countries with like-minded interests and values calling out this type of behavior, showing it has consequences, and demonstrating that it's to no one's interests for state actors to be damaging the security and prosperity of the globe and including their own citizens and companies by such reckless and indiscriminate action, as the foreign secretary has said publicly.

Stewart Baker: [00:48:06] I agree. It isn't at all clear that this is in even Russia's short-term interests. I am encouraged that a number of European states, mostly led by the UK and GCHQ, have begun attributing attacks with more confidence. That inevitably raises the question: how good do you think attribution is these days? Are you comfortable that

attributions that we're starting to see are well grounded in intelligence and could be supported if someone with clearances wanted to see the evidence?

Stewart Baker: [00:48:49] I think so, and I think the idea that attribution in cyberspace is somehow this impossible task that we shouldn't even try to get past is, I think, something that people involved in this area have moved away from some time ago. And there's a legal angle here, too. The international law and rules around attributing any kind of activity, not just cyber activity, have a role to play here. The international standards are quite pragmatic on attributing activity. And of course there are significant technical and political dimensions too, and I think we've seen advances in sort of a common understanding on each of those areas. For me the interesting bit's when you're looking at attribution internally before you even get to the question of whether you want to do anything publicly is you've got to ask these sort of basic questions. You've got to ask them: what's been happening? How did this occur? Where's it coming from? Who do you think is behind it? And crucially – and this is the one legally that can be significant in determining the parameters of your response options: *why*? And that can be quite hard, and that's where you've got to bring to bear I think in some cases decades of understanding of a particular actor's activity from a wealth of sources whether they be intelligence or open-source diplomatic reporting. And you need to act with your partners and allies, and in doing so I think through that the recent attributions of the GRU generally, the NotPetya attacks, WannaCry, we've demonstrated this can be done. And I don't think we should fear attribution. It can be difficult, at least before you start assembling the bits of information, but we in GCHQ and in the UK are far from alone in having a real wealth of expertise and experience to bring to bear on this problem.

Stewart Baker: [00:50:50] In the US we've been doing attribution a while, and the next logical step has been retribution. We've indicted – really now I think I've lost count of how many foreign intelligence officials we have indicted and indeed at least one that we have managed to arrest and extradite, although not exactly, precisely a cyber espionage agent. Should we be expecting similar actions from the UK as your attribution confidence grows?

Doug: [00:51:32] GCHQ is an organization that does work with law enforcement. It would be up to law enforcement and the independent prosecutorial authorities to decide in any given individual case or incident whether there's enough evidence to bring charges, but we have seen in a non-cyber environment the willingness of the independent investigative and prosecutorial authorities to indicate and, in the case of the Salisbury incident, a willingness to pursue criminal action. And obviously that type of ability will depend on the evidence in every given case, but the will is there should the evidence be there. And I think our country, just as in others that have independent authorities in this space, would follow the evidence where it leads.

Stewart Baker: [00:52:22] So the other thing that has happened recently is the – relative to international legal developments – is that the US has revived the United Nations [Governmental] Group of Experts [GGE] talks on the law that applies to cyber activities, the international law that applies. This time apparently they're proposing to go forward without the Russians, without the Chinese. And it was conflicts between the United States and the Russians and the Chinese that led to the collapse of GGE effort a year ago. If I remember the UK is part of those talks. Do you have an idea what kind of progress could be achieved and where in a context where there are fewer adversaries and more like-minded participants?

Doug: [00:53:21] For me I think it's worth continuing to talk about these things. What I said before was I think we've got to get to a common understanding of how the current law applies and then look at the question of whether it's enough. To me there's value in having multiple strands of communication and diplomacy on this. There's value in talking to those who are like-minded with you to form coalitions, but there's equal value in talking to those with whom you don't agree. And history has shown us a number of areas where countries with very different interests, even countries which had been in open competition or hostility in some parts of the world, came together and said, "Hey look, this is an area where we should come to some agreement that that type of activity is off limits." If you look at the early development of the law of war, for example, I think it was Tsar Alexander II who first proposed the St. Petersburg Declaration limiting the use

of exploding bullets in the 1860s. And so there's value in multiple strands of diplomatic engagement in this space.

Stewart Baker: [00:54:39] Yeah, I've often wondered whether even – certainly the Chinese and probably even the Russians you would have thought would agree that trying to bring down the financial system by attacking banks in a serious fashion. I'm not talking about intelligence collection but actually just trying to either steal money or wreck records. Just about everybody, with the possible exception of the North Koreans, the Iranians, and maybe increasingly the Russians, has a stake in a functioning international financial system. It's puzzled me, but the talks so far at GGE have focused not on trying to find sectors where there ought to be agreement not to act but more looking for principles that are more applicable but maybe less actionable.

Doug: [00:55:38] Sure. I would agree there's something in that. Maybe it's time to keep talking about the general principles and how they apply but also look at specific areas of activity where we might find more common cause, and I think it's worth a try.

Stewart Baker: [00:55:51] One thing you may not be able to answer, but I have been struck by the fact that at least the North Koreans are widely reported since they have so little Internet connectivity at home to have sent their hackers abroad. And then the question becomes: if they're operating from a third country, what can countries that have been attacked from that third country do? And of course famously in the area of terrorism, the answer is if the host country is unable or unwilling to take action to stop the attacks, then the countries that are under attack can engage in self-help. That at least has been US doctrine. I don't know whether that's UK doctrine, and I don't know that anybody has yet applied that to cyber activity. I'll give you a chance to say as much as you'd like on that topic.

Doug: [00:56:54] Well, to me it really depends on where activity has come from and what your options are in that space. So we would, our favored approach, would be to work through the most effective means possible, and that will often be in countries with well-functioning law enforcement systems to engage on that on those channels. Where

that's not possible or is unlikely to be effective, there may be other options, but we would be applying the principles of international law as set out in attorney speech. So we would think that certain activities, for example, the threat or use of force would be off the table unless one of the usual exemptions applied. We would be not looking at going past the prohibition on the non-intervention in the domestic internal affairs of a state unless we were in sort of countermeasures territory taking necessary and proportionate action in response to a prior unlawful act by that state. And then there may be other options available, including good old-fashioned diplomacy telling people, "Hey, do you know that's going on? What are you doing about it? Can we help?" So I just think you've got to look at the – it's hard to give generic, sweeping answers to this without getting into the specific circumstances of the incident and the whereabouts of the individual or groups that may be doing.

Stewart Baker: [00:58:32] So one last topic I just wanted to raise because again it indicates the differences between the US and the UK system, unusually to the advantage of GCHQ. In the US, domestic civilian cybersecurity is the responsibility of the newly named – or at least about to be named – Cybersecurity and Infrastructure Security Agency. And in the UK that responsibility falls on the National Cyber Security [Centre], the NCSC – I'm not sure what the "C" stands for – and it is very close to GCHQ in a way that the DHS is not close to NSA. Can you explain what the relationship is between NCSC and GCHQ?

Doug: [00:59:34] It's quite simply really because the NCSC, the National Cyber Security Centre, is a part of GCHQ. It's an integral core part of what we do. Well it's not – the NCSC is only coming up for two years old. That's part of our mission has been something that's been around for decades. What the NCSC does is consolidate, bring together, unite all the different bits of the British government that were looking at this, bring to bear the kind of technical expertise from all those parts of government and its agencies, the technical focus and the intelligence capabilities of GCHQ and sort of new mission to engage, to serve the government, and the British public. The sort of the aspiration is to make the UK the safest place to be online and do business online. What it's done over the past couple of years is dealt with I think over a thousand significant

incidents and many more that don't meet that threshold. A large chunk of those come from foreign state actors and the other we're looking at cybercriminals. There's been a number of initiatives to sort of engage. This isn't a solely government activity, as you and I'm sure many of your listeners well know. We're engaging with the private sector, with other bits of government, with the academic institutions, with NGOs, with individuals, and we want to bring to bear the best sort of information advice we can. The NCSC's given advice to boards on the type of questions they should be asking in sort of executing their own responsibilities in the space. It's given advice to law firms in the UK that's been welcomed by the law society. So it's out there trying to engage, and it's doing so with in a number of partnerships, including internationally. But it's very much a part of GCHQ, and that comes with – you know it's not without legal tension, but so far that's something we've been able to manage.

Stewart Baker: [01:01:46] And by and large, it's a model that has been imitated by the other English-speaking countries. We're all unique I think in having decided that cybersecurity should be divided from our signals intelligence operation, at least for the civilian sector. So usually at this point in the interview I ask our guests: so where are you going to be appearing next that people want to come meet you? But since you are at least a little undercover, you probably won't be advertising your appearances. Let me ask: is there something, some event coming up that GCHQ is releasing new materials? Are you going to attribute a few more attacks soon? Is there anything else that our listeners should be watching for?

Doug: [01:02:41] So we're sort of unusual in that we're a secret global intelligence organization, but we're trying to be as open and transparent about what we do as we can. And so there are now a number of different channels which you can hear from us, should you so choose. We have websites both for GCHQ where you can read the speeches of my director Jeremy Fleming. You can look at the NCSC website for the latest advice or announcements about incidents. The Foreign Office usually leads on external attributions. And we even have our own Twitter account, so you can sign up for that, should you be a tweeter.

Stewart Baker: [01:03:24] I apologize for not having done it. I will do it today for sure. I'll be following you. And it's been a pleasure to talk to you. I really do appreciate your openness, your willingness to discuss practically everything I asked and your engagement with the broader community on some of these issues, which I think in the long run is going to stand GCHQ in good stead. So thank you for coming in.

Doug: [01:03:55] A real pleasure. And thanks, Stewart, for these searching questions.

Stewart Baker: [01:03:59] Alright. Thanks to Doug. Thanks to Nick Weaver. Thanks to Matt Heiman for joining me. This has been Episode 235 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Be sure to send us your suggestions for future guest interviewees, and we'll send you a coveted Cyberlaw Podcast mug. Send those to CyberlawPodcast@Steptoe.com. I have begun gradually, bit by bit, putting stories that we think we'll cover on Twitter again, so if you follow @StewartBaker on Twitter or in LinkedIn, you'll start to see them. Happy to get comments on them, both substance of the story and suggestions about whether they're worth talking about. Give us a rating on iTunes, Google Play, Stitcher, Pocketcasts, whatever you use to download our podcast. We'd love to get a good review from you. Coming up we've got Chris Krebs, soon to be director of the now properly named Cyber[security] and Infrastructure Security Agency, talking about election security before the election. So we don't have much time to get that one in. And Dr. Dipayan Ghosh, the co-author of a new report, "Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet." Color me a little skeptical, so it might be an interesting exchange. And finally show credits: Laurie Paul and Christie Jorge are our producers. Doug Pickett is our audio engineer. God, I just feel so much like NPR when I do this. I love it. Michael Beaver is an intern. And I'm Stewart Baker, your host. Please join us again next week as we once again provide insights into the latest events in technology, security, privacy, and government.