

Center for Strategic and International Studies

TRANSCRIPT

Center for Strategic and International Studies

“Mitigating Security Risks to Emerging 5G Networks”

Keynote Speech

EVENT DATE

Wednesday, February 6, 2019

TIME

1:00 p.m. EST

LOCATION

CSIS Headquarters, Washington, D.C.

INTRODUCTION

James Andrew Lewis,

Senior Vice President and Director, Technology Policy Program, CSIS

KEYNOTE SPEECH:

The Honorable Jessica Rosenworcel,

Commissioner, Federal Communications Commission

Transcript by superiortranscriptions.com

James Andrew Lewis: Good afternoon. Welcome to CSIS. Our event today is “Mitigating Security Risks to Emerging 5G Networks,” a topic that continues to gain interest. We have a great panel and an amazing opening keynote speaker, Commissioner – sorry – (laughs) – Jessica Rosenworcel. I’m a little disorganized.

James Andrew Lewis: The format today will be Commissioner Rosenworcel will give opening remarks. She’ll be followed by a panel of speakers that will be moderated by CSIS Fellow Clete Johnson, Senior Fellow Clete Johnson.

James Andrew Lewis: I’m going to introduce Commissioner Rosenworcel briefly. She was named as one of Politico’s 50 politicians to watch over the next couple of years. That’s pretty impressive. She has long experience prior to serving at the FCC in telecommunications and public service, public policy.

James Andrew Lewis: Prior to joining the agency, she was the senior communications counsel for the Senate Committee on Commerce, Science and Transportation, which is really a perfect background for this stuff.

James Andrew Lewis: So we’re very fortunate to have her here to give us opening remarks today.

James Andrew Lewis: So Commissioner Rosenworcel, please. (Applause.)

Jessica Rosenworcel: Thank you, Jim, for those kind opening remarks.

Jessica Rosenworcel: And, of course, thank you to the Center for Strategic and International Studies for gathering us all here today for what is a very important conversation about security and next-generation wireless networks, known as 5G.

Jessica Rosenworcel: Now, this discussion is timely, like up to the minute. In fact, when I began thinking about how to start my remarks, I kept coming back to that familiar maxim, may you live in interesting times. And, you know, if you do a little digging online, you will find that there’s a dispute about its origin. There is one school of thought that claims it is based on an old Chinese curse. But there’s another school of thought that says may you live in interesting times; well, its provenance lies elsewhere, and perhaps with a British statesman.

Jessica Rosenworcel: Still, the more that I studied that saying and the dispute about where it came from, the more I thought that referencing it was an apt way to begin, because these are interesting times.

Jessica Rosenworcel: Last week the Department of Justice charged a Chinese equipment manufacturer and its chief financial officer with attempting to trade steal secrets, obstructing a criminal investigation, and evading economic sanctions on Iran.

Jessica Rosenworcel: Last year, in the National Defense Authorization Act, Congress prohibited executive-branch agencies from using or procuring telecommunications equipment or services from companies that are associated with or believed to be controlled by China. And in the meantime, key intelligence allies have joined us in restricting such equipment or are considering different ways to do so.

Jessica Rosenworcel: Closer to home, at the FCC, where I work, we have proposed rules that would prohibit the use of universal service funds to purchase equipment or services from companies identified as posing a national-security risk to communications networks or the communications supply chain.

Jessica Rosenworcel: So the stakes are undeniably high. That's because next-generation 5G wireless networks are, in fact, the unifying fabric that will connect us all to the future. This is the essential infrastructure for the next generation of digital technologies. It will feature data speeds 10 to 100 times higher than what we know today, and with latency reduced to as little as one millisecond. And that in turn will power autonomous vehicles, foster advances in robotics, and expand the potential for machine learning and the possibilities of the Internet of Things.

Jessica Rosenworcel: So what that means in practice is that the race to 5G is about so much more than the smartphones in our palms, pockets and purses. Those handsets represent the epicenter of the last wireless revolution, known as 4G. On its strength, we built the applications economy and changed the way we live life online.

Jessica Rosenworcel: But the coming changes with 5G are broader. Connecting the physical world around us will change everything from health care to entertainment to the way we work, and even what work entails. Plus deploying these networks promises a boost to our economy and millions of new jobs.

Jessica Rosenworcel: So it comes as no surprise that countries around the world are jockeying for position and control in this emerging ecosystem. In fact, I think the race to 5G has become a microcosm for the broader debate about global leadership and economic security.

Jessica Rosenworcel: So that's some heady stuff. And to understand it better, I think we'd actually benefit from a little bit of communications history. So let's rewind. Let's roll back to some interesting times roughly two centuries ago. That's when the British Empire dominated global communications through its undersea cable network. It was known as the All Red Line.

Jessica Rosenworcel: Now the All Red Line has a place in the history books because with such a vast empire, Britain had both the political need for cables to reach far-flung corners of the globe and the expertise needed to lay them deep on the ocean floor. And this tangle of undersea wires stretched from Ireland to Newfoundland, from Sydney to Singapore, and many more places in between. You can think of it as the Victorian internet.

Jessica Rosenworcel: Now, as a result, Britain led when it came to everything involving cable manufacture. It was an expert in cable operation. It dominated the supply of cable-building materials. Their engineers were at the forefront of electrical science, and so much so that they set the agenda for its research, dictated almost wholly by the needs of submarine telegraphy. No wonder, then, when other countries had their submarine cables built, laid, tested, and repaired, it was with British contractors and British ships. In fact, a single British cable manufacturer

known as TC&M at one point produced more than half the cables laid worldwide. Now for other nations, that leadership had consequences. It meant they were dependent on the courtesies of a foreign government for essential communications facilities even in times of war.

Jessica Rosenworcel: But in the United States, we wanted to find another way forward. We wanted communications systems that were independent. We wanted capabilities in our networks that were less susceptible to foreign control. So what did we do? In time, we invented our way to an expanded market and a more secure future.

Jessica Rosenworcel: And the spark for that future actually came in 1901, when Guglielmo Marconi famously sent the first wireless message across the Atlantic Ocean. It wasn't much. But the message, which was simply the Morse code signal for the letter S, traveled more than 2,000 miles from England to Canada. But those three clicks of Morse code were transformative, because the United States took note. It provided a way, as it evolved, to communicate with moving ships, blast messages across international borders, and bypass nationally supported telegraph monopolies. We were all in.

Jessica Rosenworcel: But the British, they determined this new technology could never challenge their dominance in cable. Well, we all know how this story ends. The All Red Line gave way to a new era of communications. The cable system dominated, by the British, was supplanted by a more diverse system of interconnected radio networks. And in the United States, we saw an inflection point in the development of communications, and we seized it.

Jessica Rosenworcel: Today, I think we are also at an inflection point. What happens with the next generation of wireless services has vast consequences for our economic and national security. The choices we make now about how these networks are deployed can result in communications technologies that are more powerful by many magnitudes. And getting them deployed early matters. It provides advantages in scale, in standards, and in device specifications.

Jessica Rosenworcel: But I believe it is no longer enough to be first to 5G. The networks we deploy must also be secure. And to build 5G security effectively, we must build a market for more secure 5G equipment. That means making sure our companies can continue to innovate and encouraging other countries to invest in 5G security, too. Now, that's a big task, and as with all significant endeavors the hard part is where to start. But I have some ideas about where the FCC should begin.

Jessica Rosenworcel: So, first, the FCC must work with other agencies to help manage supply chain risk. Late last year, the Department of Homeland Security announced the creation of the nation's first Information and Communications Technology Supply Chain Risk Management Task force. Now, that name might not fall off the tongue quickly, but that public-private partnership is going to develop recommendations to identify and manage risk in the global supply chain, and the task force includes representatives from the Department of Homeland Security as well as experts from the Department of Defense, Department of Treasury, General Services

Administration, Department of Justice, Department of Commerce, the Office of the Director of National Intelligence, and the Social Security Administration.

Jessica Rosenworcel: In addition, there is expertise brought by representatives from telecommunications carriers, equipment manufacturers, and cyber security companies. It's an impressive list, to be sure. But there is one agency that's missing. The FCC needs a seat at this table. Leaving the agency with primary oversight over communications out is neither prudent nor wise. Moreover, as I mentioned at the start, the FCC has an ongoing proceeding that speaks directly to these issues concerning equipment restrictions with the use of Universal Service Funds.

Jessica Rosenworcel: So I think good things come to those who ask and it's time for the FCC to speak up and secure a commitment from the Department of Homeland Security to participate on this task force. We should be working together. We should develop a common approach to 5G security.

Jessica Rosenworcel: Second, the FCC should charter a new 5G security council. Now, in past generations of wireless technology, it's been our practice to enjoy their benefits before fully preparing for their risk. With 4G and its predecessors, cyber security was often an afterthought. It was something to work on when deployment was substantial and it was something to manage when problems arose.

Jessica Rosenworcel: Though the capabilities of these earlier generations of wireless service really pale in comparison to those that will emerge with 5G, the vulnerabilities have been real. They range from risk with SS7 networks to the rogue use of cell site simulators. What we have learned is that retrofitting security after the fact is difficult and expensive. So I think we need a more forward-thinking approach to 5G. Cyber security needs to be front of mind.

Jessica Rosenworcel: Now, the good news is that 5G already features many security improvements over earlier generations of wireless technology. Plus, 5G standards are actually still in early days. Hundreds have yet to be developed. On standards and so much else, there is a lot of front-end work left to do, and that's where what is known as the Communications Security, Reliability and Interoperability Council comes in. The council is a federal advisory committee that provides recommendations to the FCC on high-profile security-related issues. Its two-year charter comes to an end next month and I think the FCC needs to re-charter and reinvigorate this council, and when it does, it needs to identify 5G security as its primary focus.

Jessica Rosenworcel: To this end, three things need to be a part of its mandate: more study on security technologies to mitigate the risk from the Internet of Things, more study on network function virtualization to mitigate denial of service attacks, and a new study on 5G supply chain risk management that recommends specific mitigation techniques.

Jessica Rosenworcel: And third, the FCC needs to make cyber hygiene a priority. You know, with the advent of 5G services, we are going to have wireless capability built into the

world around us. This will provide a whole new range of opportunities for civic and commercial life. But as they multiply, it will also increase our service exposure to attack.

Jessica Rosenworcel: And to prepare for this future, the FCC is going to have to expand its work to support cyber hygiene. Think of cyber hygiene in this way. To keep our communications systems functioning, we are going to need routine and regular practices that increase security and reduce exposure to risk. The agency must build these policies into its day-to-day work. Consider this: Every device that emits radio frequency at some point passes through the FCC. Go ahead. Pull out your smartphone, or your laptop, or your television. You will see on the back there is an identification number from the FCC. That stamp of approval means that the device complies with FCC rules and objectives before it is marketed and imported in the United States.

Jessica Rosenworcel: Now picture this: Going forward the number of devices could expand exponentially with 5G and the Internet of Things. So why doesn't the FCC use its equipment authorization process to encourage device manufacturers to build security into new products? To this end, it could seek to disclosure from manufacturers that explain how new devices are secure throughout the expected lifecycle of the equipment. This would support better security practices on the millions of devices headed for us with the Internet of Things.

Jessica Rosenworcel: Or, consider this, telecommunications carriers are required by the agency to certify annually that they comply with privacy standards. There is, however, no equivalent agency certification required for security. What if we changed that? What if with the next generation of wireless licenses we ask that as a condition of holding this license for public airwaves licensees will have to certify that they have implemented the best practices for 5G security. For example, we could ask that licensees certify that they are using the National Institute of Standards and Technology's cybersecurity framework. That way we ensure that licensees have a structured way of thinking about network security and a common language for managing risk.

Jessica Rosenworcel: Finally, the FCC should take steps to educate citizens on cyber hygiene. In our work, we regularly interact with consumers and consumer groups. We need to find more ways to do outreach that touch on the basics of consumer cyber hygiene, from downloading software upgrades for devices to assessing connection security when using unlicensed airwaves.

Jessica Rosenworcel: So those are my ideas for getting this conversation started. These are early days in the deployment of 5G. And, as I said at the start, they are also interesting times. But they're also the right time to ensure that communication security is front and center. Thank you. (Applause.)

(END)