Tom Wheeler served as chair of the Federal Communications Commission from 2013 to 2017. Wheeler is a visiting Fellow at the Brookings institution and senior Fellow at Harvard Kennedy school.

Billions for broadband but not a penny for cybersecurity

By TOM WHEELER AND DAVID SIMPSON
Special to The Times

Cyberattacks in the United States are getting closer and closer to catastrophic outcomes.

The headlines continually remind us that our digital infrastructure is under attack. At a time when the federal government is pouring tens of billions of dollars into internet infrastructure, cyber defense must be a required part of that expenditure.

Every one of the cyberattacks — such as the recent Colonial Pipeline and SolarWinds incursions — relied on commercial internet providers to reach

their target and do the harm. Yet, we are currently failing to use efficient regulatory mechanisms to oversee the security of these networks. The Department of Homeland Security has the expertise but lacks the regulatory authority of an agency such as the Federal Communications Commission. Yet, for the past four years, the Trump FCC was asleep at the switch, gutting cyber programs and refusing to exercise its authority.

Closing the digital divide must not create a new cyber chasm.

The tens of billions the Biden infrastructure plan has rightly proposed to connect all Americans to high-speed broadband cannot become an open door to cyberattacks. Leaving small, rural telecom operators with unsecured infrastructure and without the fiscal or human resources necessary for cyber protection is an invitation to problems. U.S.

Sen. Maria Cantwell, as chair of the Senate Commerce Committee, has identified this shortcoming and called for its resolution in the forthcoming broadband deployment plan.

We have already seen the realities of big dollar grants to small companies without cyber expectations.

Congress gave small rural wireless companies almost $2 billion to rip out their Huawei equipment — equipment, still in operation, that the government had warned wireless carriers not to buy in the first place. These small providers rationalized their risky decision on the grounds they are small, have very tight margins, and the low-priced, less complex Huawei gear seemed an easy solution. It is precisely these factors

that make such small rural companies prime targets for cyber hackers. The companies typically have fewer than 100 employees — some fewer than 10 — and often cannot afford dedicated cybersecurity personnel or cutting-edge defensive technology.

So, put yourself in the shoes of a cyber attacker. Since commercial providers are interconnected, where would you choose to launch your attack? Why target the big companies when the small internet providers have fewer protections, yet connect to all other networks? The infrastructure build-out

will create such a weak link problem if it fails to pay for and provide meaningful oversight of cyber defenses from the outset. Cybersecurity needs to be a forethought in deployment, not a bolt-on after something bad happens. Cyber risk decisions require continuous business and government engagement.

Interestingly, the president's new budget calls for a 14% increase in spending on cyber protections for nonmilitary government activities. While this will help increase the security of federal agencies, it will not move the cyber risk needle in the

commercial sectors that operate the nation's critical infrastructure connecting to those systems. It is these interconnected broadband networks that underpin our digital economy and provide the attack conduits to government, commercial and consumer targets.

Not addressing cybersecurity upfront for critical infrastructure transfers cyber risk to consumers, communities and businesses. We want high-speed digital connections for all parts of the nation to enable smart cities, smart grids, smart homes and smart business.

But the proliferation of such new activities also proliferates the number of attack vectors available to those who would do us harm. As a nation, we have been much more effective in requiring strong, audited cyber security for our defense industrial base than for the commercial networks upon which they rely. Letting the market “figure it out” will leave us with soft target links in the chain that will certainly be exploited.

In our free market economy, this is best achieved not by “federalizing” the role

of cybersecurity but by making sure cybersecurity is an essential duty for companies seeking to provide information services or products in the marketplace. The static regulatory policies of the past will no longer cut it. Because the hackers are nimble, so must be our ability to keep pace and respond.

This means creating a market oversight regime that requires the industry verticals to determine best practices, subject to regulatory oversight to make sure the solutions are fully focused and responsive.

Digital companies operate on what is called the Minimum Viable Product — MVP — approach in which a new product is introduced and constantly improved as technical and market conditions change. We need a new MVP program for cybersecurity — federal regulatory oversight built around Minimum Viable Policy that is similarly agile. In the quest to close the digital divide and regain lost momentum in the global tech economy, we can neither turn our backs on the importance of cyber protections, nor remain wedded to the

regulatory structures of the industrial era. Congress should include cybersecurity in all future critical infrastructure legislation and direct regulators to create clear expectations for cyber risk reduction through continuous and agile engagement with the companies they oversee.