Attachment —Additional Questions for the Record

The Honorable Russ Fulcher

Mr. Jaffer, on the issue of undersea cables, we have seen repeated incidents to cut or damage undersea cables that disrupts service on communication, data for business and government, as well as power and energy flows. We all know the critical role undersea cables play – $10 Tri in finance and commerce; 99% of the world's data flowing through them – most of which impacts the U.S. Several European countries around the North Sea have signed an agreement to protect critical infrastructure, Baltic countries, Finland, and others have stepped up patrolling in the Baltic Sea, and NATO is now coordinating.

1. **What do you see as next steps we can take from this Committee to ensure data flows are not interrupted?**

Jaffer Response:

There are a number of immediate steps the United States might take to ensure data flows over critically important cable infrastructure are not interrupted, some of which this Committee might work others to help accomplish. First, in the near term, our adversaries need to know that, to the extent they are engaged in efforts to intentionally cut or otherwise damage undersea cables that are critical to our national and economic security, we and our allies will take action both to protect those cables and to impose costs upon those responsible for such interference.

This Committee could support efforts to protect such infrastructure by working with other committees to authorize federal programs, through the Department of Defense and other appropriate departments and agencies—and provide incentives or funding to private entities, whether undersea cable owners and operators, insurers, or other third parties—to protect those cables, make them more resilient to attacks, and have the resources available, including repair ships, supplies, and skilled personnel, to rapidly identify attacks and reconstitute these capability, including installing devices to detect such attacks as they are underway, as well as to respond to such attacks, when directed by the President.

Likewise, this Committee could work with other committees in Congress, as well as with the President, to impose direct costs on adversaries engaged in cable attacks including but not limited to sanctions and perhaps even more aggressive responses. Given the importance of these cables, for example, it would not be out of the realm of the possible for the United States to determine that an attack on a critical cable (or cables) are the equivalent of a physical attack on the United States itself and its critical infrastructure.

Members of this Committee could also, for example, encourage the President to publicly state our nation's policy on such cable attacks, including concretely and specifically describing our plans for responding to such attacks, and also could provide the funding, support, and authority necessary to permit the President to rapidly respond, should he or she choose to do so. For such a policy to have a real deterrent effect, however, our adversaries must assess that we are both able and willing to respond. This is because without real credibility, no amount of bluster about responses will actually deter our adversaries. That means if we threaten to respond when our redlines are crossed, and those redlines are in fact crossed, we must act and we must do so publicly. For far too long our adversaries have seen an America willing to talk a big game but unwilling to actually bring it. Such behavior—which has been a problem under Presidents of both parties for well over a dozen years—does not create fear in our adversaries nor the confidence in our allies needed to achieve effective deterrence.

Finally, in the longer term, this Committee could work with industry to ensure we have backup capacity and resilient capabilities—whether using undersea cables, alternate routes, dark fiber, or satellites, among other things, to handle critical communications and to ensure that we don't suffer—once again—from a major strategic surprise when it comes to these very important capabilities.

2. **Can we look at different routes? For example, Delegate Plaskett of the Virgin Islands and I have a bill[1] that studies whether we need a new undersea cable connection between U.S. territory and Africa.**

Jaffer Response:

Certainly, alternate cable routes are a key part of building a resilient cable infrastructure that can keep communications effectively flowing, notwithstanding either intentional and inadvertent efforts that result in a cut or damage to critical infrastructure cables. Specifically, such alternate routes can help ensure that communications between the United States and our allies (and trading partners) can robustly continue even in times of natural or man-made crises.

In this case, a study of alternate cable routes like the one you and Delegate Plaskett have proposed make good sense, particularly if such a study can be completed at a reasonable cost. It may be worthwhile, while undertaking such a study, for those who either have—or are able to develop—a real knowledge base (whether prior to or as part of such a study), to look at other critical cable routes as well, and assess whether other alternatives based on cost, necessity, availability, immediate usability, and the like, might be helpful for those cable routes as well.

Of course, additional cable routes alone are not a panacea for the challenge posed by our adversaries in this domain, for a variety of reasons, including cost and time to completion, and the ability to attack those routes as well. This is why other long-term measures, including strengthening our defensive capabilities and engaging in real deterrence are also critical. Nonetheless, evaluating and establishing alternate cable routes, where appropriate, are a critical part of ensuring the resilience of our communications infrastructure and must therefore be a key part of the discussion going forward.

The Honorable August Pfluger

Multiple TP-Link Routers have been added to the NIST National Vulnerability Database for hardcoded backdoors, allowing unauthenticated remote access.

1. **Mr. Jaffer, could unsecured routers with remote access backdoors pose a national security threat to the United States? Should Americans be concerned about the security of their personal data?**

Jaffer Response:

There is no question that unsecured routers with hardcoded remote access backdoors are a massive national security—and economic security—threat to our nation and its people. And there ought be no debate whatsoever that this threat should raise significant—and immediate concerns—amongst the American people. This is particularly true given the data-hungry nature and aggressive actions already taken by key American adversaries, like the People's Republic of China.

[1] https://www.congress.gov/bill/119th-congress/house-bill/1737?s=7&r=15.

The Chinese have been for over a decade—and continue today to be— engaged in a massive spree to acquire as much data on American citizens and our allies—not just government agencies, but ordinary Americans—and to steal as much intellectual property as they can from our private sector companies. Indeed, when it comes to our people, the Chinese are building massively powerful capabilities to acquire, store, and mine the data of Americans and our allies as they seek to spread their autocratic rule and influence around the globe. These capabilities, in part powered by new and rapidly evolving artificial intelligence capabilities, require massive amounts of data to make them highly performant. Likewise, the modern Chinese economy has largely been built upon the theft of American and allied intellectual property to the tune of trillions of dollars globally.

One very effective way to acquire both data on Americans and our allies—and to steal intellectual property at speed and scale—is to own and operate the infrastructure that our communications transit over. And, if you are able to successfully build hardcoded backdoors into that infrastructure, as the Chinese government has done at scale, you have essentially written you own path to success. These Chinese have not only done this with the home and business routers you reference, but also by putting its technologies and those of its largest most capable telecommunications companies, at the heart of western telecommunications networks.

Indeed, today, our communication networks and home and business facilities are intimately laced—often to their core—with Chinese capabilities and systems that, at a minimum, could be made inoperable in a crisis, and, at worst, could serve not only as highly capable intelligence collection platforms but vehicles for the delivery of cyber weapons as well.

We must root out these systems and deploy capabilities to defend against such attacks whether targeted at our government, our private sector companies, and our citizens, and those of our allies, and we must do so rapidly.

We have seen a disturbing trend in consumer electronics coming out of China, especially when it comes to critical infrastructure technology. From ZPMC modems installed on cranes at U.S. ports, Huawei and ZTE telecommunications equipment in U.S. networks, Contec CMS8000 patient monitors in hospitals, DJI drones in our skies, and so on.

2. **What should the United States' position be when it comes to trusting technology, especially for critical infrastructure, that comes out of China? Is there a way we could tackle this issue BEFORE this technology enters our country and creates a national security risk?**

Jaffer Response:

We should not trust technology that comes out of China for any mission-critical use case, including deployment into American or allied critical infrastructure. Nor should we tolerate its use by any government agencies, whether federal, state or local, nor key private sector companies and actors particularly in critical infrastructure or related sectors. And this should be true whether those technologies are being used for law enforcement or public safety uses (e.g., in the case of DJI drones) or more ostensibly mundane uses like monitoring crops or moving cargo.

The first and most obvious way to avoid the deployment of such technology is to build robust and resilient supply chains for such technology here at home and in allied countries. This Committee can help with this effort by incentivizing investors and innovators to identify these needs in this space—partnering with the U.S. government and industry—and to build those capabilities at home and in friendly countries. This means that we must raise up our technology companies—large and small alike—and ensure they remain the envy of the world, built by the free market and free from overregulation by federal, state, and allied governments.

If we fail to offer alternatives to low-cost, often slave-labor produced, stolen-IP developed goods, that are made with government subsidies in a command-and-control economy like China, then we will continue to face a significant national security—and economic—threats from these goods and their purveyors.

But building alternative capabilities isn't enough. We have to incentivize nations around the globe as well as governments and private companies and citizens here at home to buy these capabilities, rather than investing in the cheap Chinese knockoffs or technology that come with Chinese backdoors baked in from the jump. That is, we must ensure there is broad and deep adoption of allied technology versus that of the Chinese government and its wholly owned subsidiaries in the notional private sector.

And finally, we must harden these domestic and allied technologies—from the outset and during the entire lifecycle for which they are deployed—against attacks by our adversaries, and we must also be prepared to defend ourselves, our nation, its private sector companies, and our citizens, again all manner of adversaries, including China, in both the cyber and physical domain.

The U.S. needs to do more to strengthen its position in standard-setting bodies such as the ITU. Several GAO reports have outlined issues regarding the preparatory process for forming a consensus leading up to the World Radiocommunications Conference.

3. **What changes need to be made in the preparatory process between NTIA, FCC, and the State, leading up to CITEL and the WRC? What legislative fixes should be made to streamline this process, reach a consensus earlier, and maximize the U.S. ability to deter our adversaries using the ITU to the detriment of the United States' national and economic interests?**

Jaffer Response:

There is no question that the U.S. government needs to partner more tightly with the American private sector, as well as with key private actors and governments in allied nations to make sure we get our stories straight and speak with one voice.

All too often, the federal government, or individual representatives of the federal government, are internally divided on policy, and these internal divisions—even when authoritatively resolved by the White House—breakout into the open on the international stage. This ought not be tolerated by our government, not just the White House and the President, but by Congressional leaders and key committees as well.

And even when the federal government has its act together, all too often, private sector actors are a second thought—or at least are treated as such—even in sectors like telecommunications, where the private sector plays a central, if not lead, role in key areas.

These issues are often even more of a problem for our allies. First, they often believe themselves (sometimes accurately) to be playing second fiddle to the United States, and they often have a hard time corralling or effectively coordinating with their own private sector. Moreover, they often assess the threat from key adversaries—whether China, Russia, or Iran—quite differently than we do. One only need look at the long-term reliance of Europe on Russian gas or the willingness of our allies to continue to buy obviously problematic Chinese technology, to see the very real risks in play. As a result, the United States and allies sometimes find ourselves at odds in specific policy debates even where we agree on the outcomes we seek.

If we are to effectively prevent the organizations like the ITU from becoming China-dominated and from making the same mistakes we made with certain recent technology evolutions, we must get on the same page

here at home—public and private sector alike—and we must join forces closely with our allies, convincing them to come to our view, not simply acceding to theirs.

There is no doubt that legislation might help in this domain by requiring agencies to work better together, to work more effectively with industry and allies, and requiring agreed consensus before hitting the world stage. And supporting funding for such efforts could be valuable as well. However, at the end of the day, what is critical to achieve is a shared understanding of the threat, the methods for addressing it, and accepting the reality that every day we and our allies are divided—whether the public sector from private sector or between America and European or Asian nations—we make our adversaries' work that much easier.