Military Cyber Affairs

Volume 3 | Issue 2 Article 4

December 2018

Strategy Needed to Protect National Sovereignty of US Telecommunications Backbone

Thomas Donahue
thomasjdonahue7@gmail.com

Strategy Needed to Protect National Sovereignty of US Telecommunications Backbone[1]

Thomas Donahue

The US Government—by blocking the sale of US high technology firms to foreign companies for national security reasons[2] and through trade sanctions[3] that cite unfair trade practices4—seeks to create time and space for US industry to innovate and be competitive in global markets, including those for information technology. While arguably necessary, these actions will not be sufficient to overcome a US deficit in the marketplace for high-end telecommunications integration. Overcoming this deficit will be essential not only to US economic prosperity but also to national security, which depends on telecommunications to serve as the "nervous system" for controlling critical infrastructure and military defensive systems.

The United States continues to be a source of innovation for network components at the Internet routing layer; however, the major telecommunications integration capabilities at the switching and physical layers in North America over the past two decades largely disappeared in bankruptcy or were absorbed into foreign firms as the North American firms failed to keep up with new technologies or compensate for Internet-driven commoditization and declining prices. In addition, telecommunications networks remain in flux in an extended transition from old architectures to a blend of old and new systems that vary by carrier and geography, resulting in varying degrees of capability and security across the national infrastructure.

---

[1] Please cite as: Donahue, Thomas, "Strategy Needed to Protect National Sovereignty of US Telecommunications Backbone," in Demchak, Chris C. and Benjamin Schechter, eds. Military Cyber Affairs: Systemic Cyber Defense 3, no. 2 (2018).

[2] See Treasury letter at www.qcomvalue.com/wp-content/uploads/2018/03/Letter-from-Treasury-Department-to-Broadcom-and-Qualcomm-regarding-CFIUS.pdf.

[3] See trade sanctions description at www.nytimes.com/2018/03/22/us/politics/trump-will-hit-china-with-trade-measures-as-white-house-exempts-allies-from-tariffs.html.

[4] See the March 2018 USTR Section 301 investigative findings on Chinese technology transfer, intellectual property, and innovation policies at https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

China over the same time period has developed indigenous capabilities and significant international market share, first in the developing world and now increasingly within western democracies. At first, Chinese companies were dismissed as unable to provide sophisticated, automated services that would satisfy the needs of western customers or do more than copy outdated western technology. Through the combination of persistent effort and technology appropriation efforts publicly criticized[5] by US Government officials,[6] however, Chinese companies are now poised to be top system-level and component providers for new wireless 5G networks that will increasingly represent the "last mile" for consumers of broadband services. Increasing capabilities in space launches and satellites may position China to leap ahead as well in the next generation of telecommunications (6G), which will include efforts to integrate terrestrial and space-based network elements.[7]

Aside from the economic aspects of this Chinese ascendancy, the United States also should be concerned about the long-term national security implications of an increasingly foreign, unverifiable supply chain for the nation's telecommunications infrastructure. Indeed, a mirrored concern with supply chains was undoubtedly a significant driver for China's original investment in telecommunications.[8]

A narrow technical effort to secure networks lacking trusted points of origin, distribution, and integration will fail because mitigating the supply chain threat[9] goes well beyond detecting the presence of malicious activity in individual components. The design and integration of the overall network offers more robust and stealthy opportunities to build in seemingly benign "features" that only become malicious when used in combination with targeted updates that, as part of an

[5] https://www.reuters.com/article/us-huawei-security/former-cia-boss-says-aware-of-evidence-huawei-spying-for-china-idUSBRE96I06I20130719.

[6] See the annual threat briefing by Intelligence Community leaders to Congress at www.techrepublic.com/article/us-intelligence-chiefs-say-huawei-zte-products-pose-national-security-risk/. Also see the March 2018 USTR investigative findings at https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

[7] See description of recent US industry satellite launches for telecommunications development at https://community.spiceworks.com/topic/2113457-spacex-gigabit-internet-satellites-launch-feb-22-global-service-starts-in-2019.

[8] For example, see the Notice on Issuing the "National Medium and Long-Term Science and Technology Development Plan Outline (2006-2020)" (China, State Council, Guo Fa No. 44, 26 December 2005) and the more recent Notice on Issuing "Made in China 2025" (China, State Council, Guo Fa No. 28, 7 July 2015) in which Beijing states its objective of being the "leader among the world's manufacturing powers" by 2049 in part to "protect state security".

[9] See National Institute of Standards and Technology guidance at https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management.

https://digitalcommons.usf.edu/mca/vol3/iss2/4
DOI: https://doi.org/10.5038/2378-0789.3.2.1058

integrated whole, are less likely to be flagged as problematic by inspection and testing regimes. While the theft of information could be enabled by a supply chain–induced vulnerability through traffic analysis and redirection and geolocation of individuals and sensitive facilities (not to mention direct theft of unencrypted data), the primary concern should be continuity of operations and resilience against efforts to disrupt national communications during a crisis.

In a sense, the United States now finds itself in a similar place as China was 20 years ago, albeit with a stronger cultural base of innovation. The United States must somehow *reestablish indigenous capabilities* to be used at least for the most critical national security purposes and for other critical infrastructure. To make this venture affordable, however, US companies would need to leverage and scale new capabilities to reestablish a strong position in domestic and international markets. Continuous reinvestment would be needed to preserve any recovered market share.

Telecommunications integration, however, occurs in the relatively narrow market of the telecommunications carriers rather than a broad-based consumer market, suggesting that some form of government involvement might be needed to seed a new industrial base. This seeding might seek new manufacturing methods as well as new architectures and more sophisticated components and services. Short-term strategies that only pile on new applications will not regenerate the fundamentals of the nation's backbone networks. The US Government in the past invested in the base technologies and manufacturing methods of the semiconductor (see lessons learned from Sematech[10]), battery,[11] solar energy,[12] and aerospace industries, not to mention router and other technologies that led to the development of the network originally designed for resilience against nuclear attacks, the Internet.

Focused innovation will be important but insufficient to overcome the momentum of legacy technologies and architectures now dominated by foreign companies. The US aerospace industry provides a useful case study for government seeding. The manufacturing and composite materials technology now used in modern civilian aircraft[13] were first developed decades ago for

[10] https://www.technologyreview.com/s/424786/lessons-from-sematech/.
[11] https://www.reuters.com/article/us-autos-battery-lithium/u-s-government-lab-14-firms-team-up-on-lithium-battery-idUSTRE4BH42G20081218
[12] https://www.energy.gov/eere/solar/solar-energy-technologies-office
[13] See history of military aerospace materials in https://www.scribd.com/doc/75968297/Stealth-Technology-for-Military-Aircraft-using-Composite-Materials.

US military aircraft. A similar acquisition approach by the US Government could assist trusted US industry partners acting as a consortium to deliver integrated telecommunications capabilities with performance and security embedded within new architectures for US Government national security networks and civilian critical infrastructure applications (especially industrial control systems) and ultimately for most US telecommunications backbone networks.

New architectures would need to interface with existing systems to allow for incremental adoption to spread costs over time, allow for real-world testing, and enable more rapid deployment of at least islands of secure and resilient capabilities for the most critical applications such as military command and control. However, this interface to legacy networks must not allow new systems to be undermined by the weaknesses of legacy systems.

US innovation at the component level remains strong and could feed into such a system approach to help deliver a much faster result than occurred in aerospace. Speed will be of the essence but, even so, a sustained longer-term perspective will be required measured in years and even decades, as it was for the Internet. The US Government would need to inject a national security component into the acquisition strategy—perhaps centered around hardware-based integrated technologies for encryption, authentication, and identity management—to ensure that industrial partners retain an inherent advantage in competition for US Government contracts.

This national security approach would also be essential to mitigating concerns that could be raised under international trade agreements. National security approaches, with funding from the US Government could also provide additional security for key technologies, as has been done for key military programs, to retain technical advantage at least through development and initial deployments.

Finally, the US Government would need to ensure that the partnerships, technologies, and capabilities feed into a broader commercial approach that could be sustained over the long term. Any government effort will meet resistance from many quarters if the government seeks to work in isolation. Industry has already reacted negatively[14] to reports of the US Government considering options to build a "secure 5G network." Partnerships with industry would need to include the

[14] See FCC and wireless industry criticism noted in https://www.bloomberg.com/news/articles/2018-01-29/u-s-is-said-to-consider-building-5g-network-amid-china-concerns.

https://digitalcommons.usf.edu/mca/vol3/iss2/4
DOI: https://doi.org/10.5038/2378-0789.3.2.1058

major US telecommunications carriers who do the final assembly and integration and then operate the most critical backbone networks, as well as the system manufacturers.

The United States also should consider the benefits of including key national security partners, certainly the Five Eyes, but also other western-oriented democracies with strong technical capabilities such as the Germans, the French, and the Japanese. This would also help spread the costs and open markets for the new systems in *trusted environments* and provide the critical mass needed to push through improvements in international standards.

National security and the economy require that this "backbone of democracy" be trusted and resilient. We will not succeed unless government and industry come together and reset our course. While the United States retains fundamental advantages in its broad culture of innovation and individual initiative, regaining ground in a lost industrial sector needed for a national level infrastructure will require leadership from the US Government along with sustained focus and resources. In this regard, we may have something to learn from China.