Cyberspace – the Next Utility Infrastructure

November 13, 2017 by Richard Arnold.

Note: This White Paper represents the exploratory thoughts and analysis of the author; the assertions and recommendations are provided for consideration and validation by our industry, academic, and government partners. The opinions expressed herein may not be the same as those held by the owners, investors, or other executives of CyberPoint who were not involved in the writing of this White Paper…but they should be!

Transformation to a Private-Utility Based Cyberspace

A century ago, US industry began the move from generating power as a corporate function to purchasing electricity on demand from utilities. In less than 30 years, from 1902 to 1930, the share of industrial power provided by outsourced utilities went from 0 to 80%, allowing companies to “flip the switch” for easy power, and to focus on core business. The availability of affordable, reliable power transformed US industry and the lives and habits of Americans.

Advances in information technology have transformed businesses; associated risks now demand serious attention to cybersecurity. Cheap, ubiquitous computing and storage are essential to US industry and to the lives and habits of all Americans, even as the infrastructure and operations of cyberspace become ever more complex and challenging. It was only a matter of time before information technology and cyberspace operations would move from corporate functions to general purpose capabilities purchased “on demand” from external sources. IBM’s CEO Lou Gerstner expressed his vision of Information Technology on Demand, analogous to a utility, back in December of 2000, asking “Will computing flow like electricity?” Nicholas Carr began popularizing the concept of computing as The Digital Utility as early as 2003; Carr’s *The End of Corporate Computing* was published in the spring of 2005.

It’s taken a decade for the free marketplace to generate the technology and operational capabilities to transform this vision into a reality. As companies like Amazon and Google pioneered new solutions for massive scaling of responsive, highly reliable and available computing and storage infrastructure on a national and global scale, they developed the underlying technologies and ubiquity of available infrastructure with excess capacity to move into the computing utility world – offering a variety of computing and storage services. The growth of cyber threats and high cost of continual manual updates and patches provided market opportunities for companies such as Microsoft to offer the attractive alternative of software applications services off-premises, in the “cloud” *(e.g., Office365)*.

This transformation enables companies to view IT and cyberspace operations, including cybersecurity services, as a utility characterized by high availability, automated updates, and automated network monitoring and control. These utility services are scalable and benefit from economies of scale. Delivered by trusted brand names – Google, Amazon, Microsoft, IBM, etc. – they enable pay-for-usage efficiency, provisioning by the customer, and agility to meet dynamically changing needs. Outsourcing cyber operations and cybersecurity services, functions that demand hard-to-find talent, allows company staff to focus on core business. While private-utility based cyberspace services are natural for enterprise information technology *(IT)*, they also apply to pilot, small-scale, and for some businesses even large-scale operational technology *(OT)* implementation – the networks essential to business value proposition delivery.

Unique Risks of a Private-Utility Based Cyberspace

Outsourcing engenders risks. In plugging into and relying on the power grid, you risk loss of services, degraded service quality, and high cost of change *(e.g., moving to an alternate source of power)*. Power conditioners, Uninterrupted Power Supplies *(UPS)*, backup generators, and other solutions may be required to mitigate risks to fall within an organization's tolerance. In the case of electric power, the risks and mitigating solutions are well understood. It's not as simple in cyberspace.

There are four primary areas of risks to using a private-utility based cyberspace:

1. **Technology Risks**. Unlike the power grid, where many elements of the infrastructure can remain constant for a decade or more, the technology underlying utility cyberspace services is dynamic, with technology refresh cycles of 3 - 5 years and new features and functions popping up twice as fast. Solutions thought secure, such as mixed trust virtualization, may be susceptible to resource misuse, starvation, or theft. The spectrum of cyber threats and available cybersecurity solutions changes daily.
2. **Barriers to Change**. Well-honed procedures for provisioning, continuous business operations, and the high cost of data migration and parallel transition operations impose high barriers to change once a private-utility provider is selected and business operations become reliant on that utility. Effective vendor lock-in, and the potential for price abuse, is real. And unilateral vendor infrastructure changes may "break" mission critical operations flow with devastating consequences.
3. **Self-inflicted Wounds**. Contrary to a power utility – where a customer's influence is constrained to a well-defined physical interface and perhaps coordinating control / information sharing – a customer generally stores data and or applications programs within the cyberspace utility infrastructure. User email handling on a virtual machine in the utility infrastructure, for example, may result in successful spear-phishing or ransomware adversary operations that lead to security compromises or devastating conditions *(e.g., adversary encryption of all files)*. With power, the ability to suffer self-inflicted wounds is restricted to a small set of trained experts; with cyber, all users are capable of inflicting devastating wounds.
4. **Service and Pricing Validation**. How does a buyer know that the services are actually being delivered at or exceeding the agreed service levels? This is especially challenging

regarding outsourced cybersecurity services, either from the utility vendor or an external third party. Absence of notification of threat attempts to exploit or attack does not prove the absence of attack; at the extreme, if a cybersecurity service provider simply sends an email "no attacks got through!" but did no actual monitoring, how would you know? Finally, given the complexity of service delivery and pricing models, how do you know if the current pricing is "fair," or if as a long-time customer subject to vendor lock-in you are being unfairly price-gouged?

Cyberspace Utility Infrastructure and the Infrastructure Initiative

Cyberspace services, including cybersecurity, are essential to modern American business operations. They are also considered essential to daily lives by most Americans, who expect and rely on constant connectivity and use of the thousands of apps that enhance so many aspects of daily life.

As the Trump Administration develops and executes plans to modernize the infrastructures of our nation to prepare us for decades of rapid growth – the Infrastructure Initiative – those plans and programs should include the nascent and burgeoning cyberspace outsourced-services infrastructures, e.g., the cloud-based automated information processing and storage services, including Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service, Cybersecurity-as-a-Service, etc.

As these services become more used across the commercial world and by private citizens, they may qualify as a new component of the Information Technology Critical Infrastructure upon which our nation depends. Companies, including many of the small businesses we intend to rely on to fuel economic growth, increasingly depend upon these private-utility services for operations.

Critical questions to be explored include:

- Are there sufficient safeguards to protect these consumers of services from unfair business practices or devastating unilateral changes backed up by fine print in service level agreements that don't take into account the unfair advantage of behemoth providers who are used to "sign up as is or don't use" software license agreements?
- Is the cyberspace services industry sufficiently regulated to ensure that those private companies who ask for and are given the trust of so much critical infrastructure have the assets and plans to fulfill their commitments and live up to that trust?
- People trust in regulatory officials to ensure the pricing of electricity from utilities is fair and reasonable. Given that cyberspace services provided as a "utility" are enabled by and benefit directly by increasing economies of scale, are checks and balances in place to ensure that future effective monopolies or oligopolies are providing fair and reasonable prices? Given the high costs of transitioning from one provider to another, are checks and balances in place to ensure services are not degrading or becoming obsolete for those customers effectively locked in?

- Are there business models and supporting regulatory infrastructure that can help mitigate the unique risks of a private-utility based cyberspace? For example, should critical infrastructures that use private-utility based cyberspace be required to engage independent third parties to test/validate that utilities are meeting their service level agreements?

We can see the future. Cyberspace utility services are a key part of our nation's infrastructure, and will continue to grow in importance. They allow businesses to focus on core business, treating information technology as an outsourced, general purpose technology and tool. Achieving economies of scale through transformation into a utility enables efficient use of our limited IT and cybersecurity resources – we'll have enough people to do those jobs right. Cyberspace utility services have the power to transform America and open up new opportunities, just as electric utility services did a century ago.

Now is the time to include cyberspace utilities in the Infrastructure Initiative, to ask and explore critical questions and determine appropriate national policy. The technology and business models are proven. Usage is about to explode. And with the Infrastructure Initiative, we have the chance to get this right!