TRUSTWORTHY & RESILIENT CYBER SYSTEMS SECURITY REVIEW

The U.S. national cyber systems infrastructure is comprised of the following system components: (1) manufactured computer hardware; (2) manufactured and custom computer software; (3) network servers, routers, and software; (4) the network infrastructure including satellites, land lines, switching stations and data messaging protocols; (5) various levels of information services (IS) and network administration; (6) human operators; (7) human and machine receivers of data produced by the system; and (8) data stores that include the hardware, software and the stored data accessible to the cyber system. This cyber systems infrastructure has been built-up piecemeal over the past 40 years, with the primary growth in the system over the past 20 years. To be trustworthy and resilient to collapse, each system component must be maintained and regularly replaced by a new upgrade of the system component (e.g. moving from IPv4 to IPv6 minimum Internet protocols; 64-bit chip/OS architecture). Human operators require ongoing training to be able to operate the cyber systems infrastructure securely.

THE PRIMARY SOURCES OF INSECURE CYBER SYSTEMS

The estimated ongoing operating and maintenance (O&M) costs and repair and replacement (R&R) costs for the nation's cyber infrastructure is $248 billion annually.[1] On an annual basis, the deferred O&M and R&R costs are approximately $126 billion. The size and ongoing nature of these deferred investments in adequate O&M and R&R result in a highly vulnerable system that is prone to compromise and partial system collapse for a variety of known and unknown factors. Probabilistic annualized threat estimates of partial cyber system collapse from mishaps due to human error 40%; deliberate attack of the national infrastructure 30%; and emergent causes (black swans) are 20%.[2] Sources of threats to the national infrastructure are global.

CYBER SYSTEMS SECURITY REVIEW FINDINGS

- The network configuration (e.g. Internet or intranet connectivity) is not necessarily the most vulnerable component of the U.S. cyber systems infrastructure. Total system vulnerability results from the combination of the probability for disruption from each component of the system. With their contributions to a probabilistic forecast of system disruption, human operators, manufactured and custom computer software, and manufactured computer hardware each contribute more relative vulnerability than does the network infrastructure. Human operators often are inadequately trained and do not routinely perform even minimal ongoing O&M to the software and hardware under their control or use. Even with adequate O&M, some hardware and software is so out-of-date due to lack of timely R&R, that adequate security cannot be maintained. The fact that this outdated hardware and/or software is connected to the network and that human operators may not address even minimal O&M requirements creates a situation of heightened vulnerability to other network users whether this is a highly secured or unsecured network.

- Lack of adequate investments in O&M and R&R are the primary limiting factors for protecting the nation's cyber infrastructure from mishaps, deliberate attacks, and collapses. The opportunity cost of not making these annualized investments in adequate O&M and R&R may result in an Incremental Capital Output Ratio (ICOR) that equates to a loss of about $500 billion in GDP annually, on average.[3]

- There is a statistically higher probability for catastrophic damage to sectors of the nation's economy from cyber system infrastructure collapse due to inadvertent system failures than in deliberate malicious attacks against the national cyber systems infrastructure.

---

[1] All numbers in this draft are placeholders, requiring additional analytical work for accuracy.

[2] Emergent behavior is difficult to predict from an analysis of the system and its components.

[3] A metric that measures the marginal amount of investment capital necessary for an improvement in the national economy's level of production efficiency.

- Network vulnerability is exacerbated by out-of-date computer hardware, routers, and operating system software being connected via an Internet based on out-of-date data messaging protocols, user anonymity, and often user-choice of level of network security engaged. Thus, practically speaking, the network's vulnerability is often determined by the lowest common denominator of capabilities determined by out-of-date computer hardware, routers, operating system software, end-user training, and Internet messaging protocols.

- The single greatest bang-for-the-buck from a cyber systems infrastructure perspective would be to upgrade minimum Internet data messaging protocols to IPv6. However, with this Internet upgrade all computers and routers connected to the Internet should be required to be minimum 64 bit chip/operating system architectures. It is unlikely that for the foreseeable future an affordable one-time fix to the national cyber systems infrastructure's vulnerabilities will be found. Successive waves of new technology will be required to stay ahead of the curve to prevent inadvertent system failures and collapses due malicious attacks. Maintaining a less vulnerable national cyber system infrastructure requires the capability and intension to rapidly adopt new technology and maintain minimum network connectivity standards. Normal new technology adoption cycles are typically 15-30 years. A great deal of additional security could be established if these technology adoption cycles were reduced to 7-10 years for system components of the national cyber systems infrastructure.

- However, the inherent vulnerabilities of the U.S. national electricity grid to withstand powerful solar storms[4] and EMP (electromagnetic pulse) attack[5] disruption or shutdown due to inherent system design limitations, as well as from human error introduces another significant level of risk.[6] The national cyber system infrastructure relies on clean, dependable electricity sources to function at all.

RECOMMENDATIONS TO UPGRADE THE SECURITY OF THE NATIONAL CYBER SYSTEM INFRASTRUCTURE

- Implement the *National Unified Smart Grid Initiative*. This will bring the U.S. electricity grid up to standards necessary to withstand powerful solar storms and EMP (electromagnetic pulse) attack disruption or shutdown, to reduce transmission losses, and to enable lower EROI (energy return on investment) energy sources that reduce GHG (greenhouse gas) emissions to be connected to the national grid.

- Set up a national *Internet Connectivity Registry* and require an annual connectivity fee be paid either by user or by connection device. Set standards for all Internet connectivity, e.g. require all connection devices to be capable of IPv6 data protocol operations. Provide rebates of the annual connectivity fee to all users who upgrade their hardware and software to IPv6 compatibility. Every two years, add additional connectivity standards that reduce system vulnerabilities. Continue to provide connectivity fee rebates to those users who upgrade their cyber systems technology.

- Set up the National Cyber Systems Threat Center in the ODNI to set standards and fees.

---

[4] The consequences of a future solar storm like the Carrington Event of August-September 1859 are extensive and involve a range of potential economic impacts not unlike a major Force 5 hurricane or tsunami that could cripple the present national electricity grid for an extended period. See National Research Council, "Severe Space Weather Events--Understanding Societal and Economic Impacts Workshop Report" (NASA, 2008).

[5] See Dr. William R. Graham, et. al., "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume 1: Executive Report (2004)."

[6] The national grid, 164,000 miles of high-voltage transmission lines and 5,000 local distribution networks is outdated, highly vulnerable, inefficient, and unsuitable for fluctuating renewable power sources.