Computing and Cyber Tools

Emerging cyber tools and computational capabilities will expand and connect the digital world in ways that will create new opportunities as well as new cybersecurity vulnerabilities. Quantum information sciences (QIS), the Internet of Things and cloud computing are among the most promising technologies in terms of impact on the evolution of the digital world — and potential for proliferation.

Quantum Information Sciences

Quantum information sciences (QIS) is an interdisciplinary field at the intersection of quantum mechanics and computer and information sciences. QIS seeks to understand how information is processed and transmitted using quantum mechanical principles and develop new forms of computing and information processing that surpass classical limitations. It is the exploitation of quantum properties for the storage, transmission, manipulation, computing, or measurement of information. Though there are many disciplines within the QIS field, it comprises three primary subfields: quantum computing, quantum sensing and quantum communications.

- **Quantum computing** uses quantum physics to solve problems at speeds not possible with classical computers by exploiting the superposition of quantum bits (qubits). Qubits are capable of holding exponentially more information than traditional bits and can be manipulated to solve the kinds of difficult problems simply not possible with traditional computers.
- **Quantum sensing** is advanced sensor technology capable of improving measurement, navigation, exploration, observation, and interaction with physical objects and material. It exploits quantum phenomena to capture extremely precise and highly sensitive measurements at the atomic level.
- **Quantum communications** applies the properties of quantum physics to better secure long-distance communications. It uses photons to transmit qubits between remote destinations and protects information against eavesdropping by means of quantum cryptography. The most well-known and developed application of quantum cryptography is quantum key distribution (QKD). QKD describes the use of quantum mechanical effects to perform cryptographic tasks or to break cryptographic systems.

QIS Proliferation Concerns

Like artificial intelligence, the nature of QIS's impact on proliferation will be determined by how it is ultimately combined with developments in other scientific and technological disciplines. Most advanced quantum capabilities will not be fully mature in the near term, but developments in quantum sensing and quantum communications could prove particularly destabilizing. For example, highly sensitive nuclear secrets will become more vulnerable in a post-quantum cryptography world where communications and information are susceptible to decryption. Moreover, quantum sensing has direct military application through improved detection and geolocation of highly faint, highly sensitive objects — such as ballistic missile submarines.

Internet of Things

The Internet of Things (IoT) refers to a network of wirelessly connected objects that are able to communicate, respond to and synchronize functions through the use of integrated sensors and software. These devices, known as "smart objects," can range from simple devices like smart thermostats, to wearables like smartwatches and RFID-enabled clothing, to complex industrial machinery and transportation systems. It is the interconnection through the internet of electronic objects, both traditional computer systems and non-computer systems, to communicate, share data and improve performance all without human intervention.

IOT Proliferation Concerns

The creation of an IoT, even a privately segregated IoT accessible only to a credentialed group, poses cybersecurity risks that could expose sensitive information. The more devices that are connected to a network, the greater the number of potential access points for malicious actors to gain access to private data. Moreover, devices and systems not previously "connected" often have security, operability and performance issues when being upgraded to an IoT connected state. Many systems were not designed to interact remotely with unauthorized users and lack adequate security protocols. For example, to improve performance and output, a nuclear enrichment plant may upgrade its facilities to a secure IoT. This would require connecting legacy machinery with state-of-the-art computer processors, advanced wireless telecommunications networks and utility conduits that extend outside the perimeter of the facility. This will create multiple vulnerabilities at each of these nodes that could be exploited. Additionally, it could require connecting previously independent record systems with weak protection to new industrial equipment that could be sabotaged remotely if access is gained by exploiting incompatible security protocols. In essence, by connecting entire enterprises and enabling remote access, the risk of a catastrophic failure can increase.

Cloud Computing

Cloud computing can be thought of as on-demand access to Internet services. These services can include data storage, software, analytics, networking and more. A cloud network is a collection of remote servers hosted on the Internet to record, store, and manage data, as opposed to holding it on local servers. Cloud computing offers access to information from anywhere in the world there is an Internet connection and can be set up as both public and private networks. It has emerged as a competing cost and operating model to the traditional IT infrastructure heavy model.

Cloud Computing Proliferation Concerns

Like other remote access technologies, cloud computing raises cybersecurity concerns. As part of NNSA's modernization efforts, for example, it is prioritizing cloud adoption and hoping to deploy commercial cloud-based technologies for classified data. NNSA's computer modeling of weapons design and stockpile testing data must be available across the DoD community and remotely accessible to NNSA employees. Cloud computing introduces vulnerabilities by way of increasing the attack surface of an enterprise, meaning adversaries have more potential access points. Third-party vendors that store and facilitate access to data also may not have as stringent security measures as necessary to protect against capable cyber actors. As an agency such as NNSA scales up its use of cloud storage, cybersecurity risk management becomes essential to protecting sensitive information from cyberattacks. The process of migrating to the cloud can be a lengthy effort during which enterprises remain particularly vulnerable. Findings from an audit of the Nuclear Regulatory Commission's adoption of cloud computing, for instance, revealed this can hamper network security.