Cyberspace operations offer unique military challenges. The paragraphs below address some of the known challenges: mission assurance, a compressed decision cycle, anonymity and the attribution challenge, and various threats inherent to cyberspace itself.

There is a requirement to balance defensive cyberspace actions within cyberspace with their impact on ongoing air, space, and cyberspace operations. The lack of situational awareness among domains can cause serious disconnects in one, significantly hindering operations in others.¹

Mission Assurance

Mission assurance consists of measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions (MEFs), mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities.²

Mission assurance ensures the availability of a secured network to support military operations by assuring and defending the portion of the network directly supporting the operation. Cyberspace mission assurance begins by mapping the operation to the supporting architecture. Then, deliberate actions are taken to assure the availability of that portion of the network. These may include adding backups to single points of failure in the network or delaying certain maintenance actions to ensure the network will meet mission requirements. Second, the proactive actions are taken to ensure the network is secure and defended. These actions may include focusing the attention of defensive cyberspace operations assets on the slice of the network supporting the operations and conducting operations to ensure no threats are resident on the network.

A “contested cyber environment” involves circumstances in which one or more adversaries attempt to change the outcome of a mission by denying, degrading, disrupting, or destroying our cyber capabilities, or by altering the usage, product, or our

confidence in those capabilities.³

Warfighters should realize risks and vulnerabilities are often created by the interdependencies inherent in the networking and integration of systems through cyberspace. Integration of cyberspace operations involves actions taken to enable decision superiority through command and control (C2), innovation, integration, and standardization of systems across air, space, and cyberspace domains. Integration means are tested via operational experiments like the Joint Expeditionary Force Experiment. Identifying vulnerabilities is difficult within a contested cyber environment. Our systems are open to assault and are difficult to defend. Some known examples of vulnerabilities in cyberspace operations are listed in the National Military Strategy for Cyberspace Operations (NMS-CO).

Assuring missions via cyberspace operations involves risk. Since the nature of cyberspace is interconnectivity, all cyberspace operations have inherent risk requiring constant attention and mitigation. Cyberspace is a domain with its own set of risks. In this domain, a risk assumed by one is potentially assumed by all. Mitigation of risk can result in a decreased risk level considered acceptable to continue conducting operations.⁴ Examples of this kind of approach toward handling risk can be seen in many aspects. The implementation of firewalls, training, education, and intrusion detection and prevention systems represent types of risk mitigation.

Just as in the air domain, we do not defend the entire Cyberspace domain; we defend what is relevant to our operations. In cyberspace, this means protecting pathways and components, since action against critical systems could seriously degrade our ability to fight and win. Whether used offensively or defensively, however, conducting particular cyberspace operations may require access to only a very small “slice” of the domain. This does not mean “localized” in the sense of a limited geographical area (although that too may sometimes be required), but perhaps just a string of internet protocol (IP) addresses, which may span the globe but represent only a miniscule portion of data flow bandwidth. Similarly, it may involve the ability to hack through one particular firewall that may physically reside upon several servers, but which is never engaged physically only through virtual means. Finally, many operations may span only seconds from inception to conclusion, given the speed at which the Internet operates. Successfully operating in cyberspace may require abandoning common assumptions concerning time and space.

Freedom of action in cyberspace is a basic requirement for mission assurance. However, having the cyberspace capacity to achieve this freedom of action should not be taken for granted. Just as operating in the air domain requires having the capacity to

---
³ Ibid.
do so (airborne platforms, runways, etc.), the Air Force should ensure it acquires sufficient capacity (bandwidth, components, etc.) to operate within cyberspace. Since access to cyberspace permeates daily activities, it is easy to overlook this requirement and assume that sufficient capacity will simply exist.

Cyberspace operations seek to ensure freedom of action across all domains for US forces and allies, and deny that same freedom to adversaries. Specifically, cyberspace operations overcome the limitations of distance, time, and physical barriers present in other domains. Exploiting improved technologies makes it possible to enhance the Air Force’s global operations by delivering larger information payloads and increasingly sophisticated effects. Cyberspace links operations in other domains thus facilitating interdependent defensive, exploitative, and offensive operations to achieve situational advantage.

Potential adversaries wish to undermine mission assurance actions via cyberspace operations. The Air Force ensures it can establish and maintain cyberspace superiority and fight through cyberspace attacks at any time regardless if the US requires the use of military forces. Our adversaries have also demonstrated that they can create civil instability through cyber attacks. The Air Force maintains a capability to provide defense support to civil authorities in cyberspace when called upon by national leadership. Potential adversaries have declared and demonstrated their intent; Russia’s relatively crude ground offensive into Georgia in 2008 was preceded by a widespread and well-coordinated cyberspace attack. The massive cyberspace attack and ensuing effects suffered by Estonia in 2007 illustrate how quickly malicious hackers affect even a technologically sophisticated government.

One last point to highlight concerning mission assurance is homeland infrastructure protection from threats or natural disaster. The Air Force should prepare to respond rapidly to mitigate effects of such threats or events and reconstitute lost critical infrastructure capabilities while also providing support to civil authorities as directed by competent authority. The Air Force should establish policies and guidance to ensure the execution of mission essential functions for critical infrastructure protection, in the event that an emergency threatens or incapacitates operations.

**Compressed Decision Cycle of Cyberspace Operations**

The fact that operations can take place nearly instantaneously requires the formulation of appropriate responses to potential cyberspace attacks within legal and policy constraints. The compressed decision cycle may require predetermined rules for [intelligence, surveillance, and reconnaissance](https://en.wikipedia.org/wiki/Intelligence,_surveillance,_and_reconnaissance) (ISR) actions.
Anonymity and the Inherent Attribution Challenge

Perhaps the most challenging aspect of attribution of actions in cyberspace is connecting a cyberspace actor or action to an actual, real-world agent (be it individual or state actor) with sufficient confidence and verifiability to inform decision- and policy-makers. Often this involves significant analysis and collaboration with other, non-cyberspace agencies or organizations. While cyberspace attribution (e.g., identifying a particular IP address) may be enough for some actions, such as establishing access lists (e.g., “white” or “black” lists of allowed or blocked IP addresses), attribution equating to positive identification of the IP address holder may be required for others, such as offensive actions targeting identified IP addresses.

The nature of cyberspace, government policies, and international laws and treaties make it very difficult to determine the origin of a cyberspace attack. The ability to hide the source of an attack makes it difficult to connect an attack with an attacker within the cyberspace domain. The design of the Internet lends itself to anonymity.

Anonymity is maintained both by the massive volume of information flowing through the networks, and by features that allow users to cloak their identity and activities. Nations can do little to combat the anonymity their adversaries exploit in cyberspace; however, the same features used by terrorists, hackers, and criminals, strengthen state surveillance and law enforcement capability, in modified form. Actions of anonymous or unidentified actors are akin to an arms race. Illicit actors continually amaze those in global law enforcement with the speed at which they stay one step ahead in the technology race. Nevertheless, nations have the advantage of law and the ability to modify the technological environment by regulation.

Anonymity is a feature of the Internet because of the way information moves through it and the way it is governed. The underlying architecture was intended to be robust, distributed, and survivable. The anonymous nature of the Internet is literally written into the structure of the Internet itself and cannot be dislodged without physically destroying many networks. The Internet was also designed where the intelligence was placed at the ends of the network, not in the network itself. Routing tools, software applications, and information requests come from the ends, in contrast to a traditional telephone network in which the switches, routing protocols, etc., are in the network itself. The difference makes it much harder to trace individual bits of information once they are in the network. The Internet’s governance structure reflects its design.5 This makes attribution a challenge.

5 Ibid.