According to NIST, cybersecurity (CS) is generally treated as a subset of information security (IS), aligning with your view.

NIST Definitions

Information Security (IS):
"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide **confidentiality, integrity, and availability**."

This is the foundational definition, drawn from laws like 44 U.S.C., Sec. 3542 and standards like FIPS 200. It covers information in *any form* — digital, paper, verbal, etc. — and includes physical, administrative, and technical protections.

Cybersecurity (CS):
NIST provides several closely related definitions, including:

- "The ability to protect or defend the use of **cyberspace** from cyber attacks."
- "Prevention of damage to, protection of, and restoration of computers, electronic communications systems... including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

Cybersecurity focuses specifically on the *digital/cyber domain* — networks, computers, electronic systems, and data in cyberspace.

The Relationship

NIST treats **information security as the broader umbrella** that encompasses cybersecurity along with other areas like physical security, personnel security, and protections for non-digital information. Cybersecurity is the portion of information security dedicated to defending against threats in cyberspace.

This relationship is reflected in:

- NIST's **Computer Security Resource Center (CSRC)**, which covers both but frames much of its work under the umbrella of information security.
- Documents like NIST SP 800-12 (*An Introduction to Information Security*), which discusses information security principles while addressing cyber elements.

- The **NIST Cybersecurity Framework (CSF)**, which focuses on managing *cybersecurity risk* as part of broader organizational risk management (often within an information security program).

In practice, NIST publications often use the terms in ways that show significant overlap, especially since most modern information exists in digital form. However, the formal distinction holds: IS is broader.

Your interpretation (CS ⊂ IS) matches the common understanding in NIST-aligned sources and industry consensus. Other interpretations (e.g., treating them as largely synonymous in casual usage) exist, but NIST's definitions and structure support the subset relationship.