Fact Sheet: *2023 DoD Cyber Strategy*

This week, the Department of Defense (DoD) transmitted to Congress the classified *2023 DoD Cyber Strategy.* The *2023 DoD Cyber Strategy* establishes how the Department will operate in and through cyberspace to protect the American people and advance the defense priorities of the United States.

This strategy is subordinate to the *2022 National Security Strategy* and the *2022 National Defense Strategy.* It complements the *2023 National Cybersecurity Strategy* and builds upon and supersedes the *2018 DoD Cyber Strategy.* An unclassified summary is forthcoming.

The *2023 DoD Cyber Strategy* is grounded in real-world experience. Since 2018, the Department has conducted a number of significant cyberspace operations through its policy of defending forward, actively disrupting malicious cyber activity before it can affect the U.S. Homeland. This strategy is further informed by Russia's 2022 invasion of Ukraine, which has demonstrated how cyber capabilities may be used in large-scale conventional conflict.

These experiences have shaped the Department's approach to the cyber domain:

- The Department will maximize its cyber capabilities in support of **integrated deterrence,** employing cyberspace operations in concert with other instruments of national power.
- The Department will **campaign** in and through cyberspace below the level of armed conflict to reinforce deterrence and frustrate adversaries.
- Finally, the Department recognizes that the United States' **global network of Allies and partners** represents a foundational advantage in the cyber domain that must be protected and reinforced.

The Department confronts an increasingly contested cyberspace:

- **The People's Republic of China (PRC)** represents the Department's pacing challenge in the cyber domain. The PRC has made significant investments in military cyber capabilities and empowered a number of proxy organizations to pursue malicious cyber activities against the United States.
- **Russia** poses an acute threat in cyberspace, evidenced by its malign influence efforts against the United States and repeated cyber attacks against Ukrainian civilian critical infrastructure.
- **North Korea, Iran, and Violent Extremist Organizations** remain persistent cyber threats.
- **Transnational Criminal Organizations** represent a unique threat in cyberspace due to their technical aptitude and often close alignment with the foreign policy objectives of their host governments.

In order to address current and future cyber threats, the Department will pursue four complementary lines of effort:

- **Defend the Nation.** The Department will campaign in and through cyberspace to generate insights about malicious cyber actors, as well as defend forward to disrupt and degrade these actors' capabilities and supporting ecosystems. Additionally, DoD will work with its interagency partners to leverage all available authorities to enable the cyber resilience of U.S. critical infrastructure and to counter threats to military readiness.

- **Prepare to Fight and Win the Nation's Wars.** The Department will ensure the cybersecurity of the DoD Information Network and will further invest in the Joint Force's cyber resilience. Additionally, the Department will use cyberspace operations to generate asymmetric advantages in support of the Joint Force's plans and operations.
- **Protect the Cyber Domain with Allies and Partners.** The Department will assist U.S. Allies and partners in building their cyber capacity and capability, as well as expand avenues of potential cyber cooperation. DoD will continue to conduct hunt forward operations to build cyber resiliency and will reinforce responsible state behavior by encouraging adherence to international law and internationally recognized cyberspace norms.
- **Build Enduring Advantages in Cyberspace.** The Department will optimize the organizing, training, and equipping of the Cyber Operations Forces and Service-retained cyber forces. Furthermore, DoD will invest in the enablers of cyberspace operations, including intelligence, science and technology, cybersecurity, and culture.

With a robust and integrated cyber capability, the Department will work to deter conflict where it can and prevail where it must.