Joint STATEMENT FOR THE RECORD of
Mr. Christopher Maier, Acting Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict,
Mr. Neill Tipton, Director of Defense Intelligence (Collections and Special Programs), and
Mr. James Sullivan, Defense Intelligence Officer for Cyber, Defense Intelligence Agency
before the
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS
on
"DISINFORMATION IN THE GRAY ZONE: OPPORTUNITIES, LIMITATIONS, CHALLENGES"

March 16, 2021

(U) Chairman Gallego, Ranking Member Kelly, and distinguished committee members, it is an honor to be with you today.

(U) We are here today to discuss the impact of "disinformation in the gray zone" and the Department of Defense (DoD) efforts to maintain the operational advantage in this evolving threat environment.

(U) The DoD understands "disinformation" to consist of the deliberate dissemination of false information with the intent to deceive. Examples include planting false news stories in the media, false narratives in social media, and tampering with private and/or classified communications before their widespread release. Disinformation is also closely related to misinformation, which can be defined as the unintentional dissemination of false information, for example, internet trolls who spread unfounded conspiracy theories or web hoaxes through social media, believing them to be true. "Disinformation" and "misinformation" both exploit false information. Effective false information is usually crafted from a kernel of truth, deliberatively manipulated with false information or selective omission of true context. The deliberate employment of mis- and disinformation can be considered in the execution of propaganda. Propaganda is the

dissemination of an idea or narrative that is intended to influence. It may be misleading or true. An actor or government communicating its intent, policies, and values through speeches, press releases, and other public means can be considered propaganda.

(U) Adversary use of disinformation, misinformation, and propaganda poses one of today's greatest challenges to the United States, not just to DoD. Russia and China, as well as non-state actors, understand that in today's information environment they have real-time access to a global audience. With first-mover advantage and by flooding the information environment with deliberately manipulated information, i.e., mostly truthful with carefully crafted deceptive elements, these actors can gain leverage to threaten our interests.

(U) Russia sees the information sphere as a key domain for modern military conflict. Russia has prioritized the development of forces and means for information confrontation in a holistic concept for ensuring information superiority since at least the 1920s. Russia wages this struggle for information dominance during peacetime and armed conflict with equal intensity using combined electronic and kinetic means and methods through information-technical, information-psychological, and active measures. The Russian Government claims NATO countries, led by the United States, have created a powerful information operations (IO) system and are expanding and improving it.

(U) Russia sees the Information Domain differently than the United States and its allies and partners. Russian publications and actions indicate its government maintains a holistic concept of "information confrontation" ("informatsionnoye protivoborstvo"). Specifically, "information confrontation" seeks to dominate the Information Domain through a combination of what it defines as information-technical effects -- or means that seek to manipulate networks, computers and data -- and information-psychological effects all intended to target people or a population to influence behavior or opinions. We are increasingly seeing the integrated use of cyber-enabled psychological actions, distributed denial of service attacks, propaganda disseminated through social media and bots, strategic deception and disinformation, and electromagnetic warfare to achieve strategic goals.

(U) China seeks to influence domestic, foreign, and multilateral political establishments and public opinion to accept China's narratives and to remove obstacles that prevent China from attaining its goals, including the sustainment of the Communist Party regime. The People's Liberation Army (PLA) has developed the concept of "Three Warfares" – public opinion, legal, and psychological warfare -- as key components of its psychological-cognitive warfare efforts. These efforts are designed to demoralize adversaries and to influence foreign and domestic public opinions.

(U) Similar to Russia, China also takes a broad approach including the establishment of a state-directed global media network, overt and covert ties to Mandarin-language media in third countries, and the employment of cyber techniques. China views the cyber domain in particular as an ideal platform for strategic influence and deception and disinformation operations. The PLA likely seeks to use digital influence activities to support its overall "Three Warfares" concept and to undermine an adversary's social cohesion, economy, morale, and governance. These operations are conducted with equal intensity in peacetime and during armed conflict. The PLA goals for social media influence activities fall into broad categories: promote a narrative favorable to China, undermine adversary resolve and social cohesion, shape foreign governments' policies in favor of China's core interests

(U) Although we are here today to discuss various DoD efforts, we recognize that we do not have a monopoly on U.S. Government capabilities to combat disinformation, nor should we; the DoD is one part of a whole-of-government approach to this challenge, and other civilian departments and agencies have critical roles and responsibilities, which demand close interagency coordination and clear authorities. Disinformation contributes to an environment in which consumers of information trust no one. The United States and our allies and partners must continue to counter disinformation by exposing the lies and their sources, and providing factual information from trusted transparent sources. Coordinated interagency effects can complement the efforts of each department or agency to defend the nation against disinformation and to reach and engage global audiences.

(U) As we strive to leverage DoD's information operations capabilities in competition with malign actors, we first acknowledge – as reiterated in the recently published Interim National Security Strategic Guidance – that we will actively support elevating diplomacy as our tool of first resort. DoD will directly support and coordinate with the Department of State's Public Affairs and Public Diplomacy teams and the Global Engagement Center, as well as complement the U.S. Agency for Global Media operations.

(U) In addition, DoD will address the tasks required in Section 1631 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2020 to improve integration of policy, strategy, planning, resource management, operational considerations, personnel, and technology development across all the elements of information operations of DoD. The Secretary has designated a Principal Information Operations Advisor (PIOA) and will build a cross-functional team to assist in the accomplishment of the POIA's primary responsibilities. We have initiated the required Information Operations posture review, and that includes reviewing how the DoD is organized and is evolving to ensure we successfully execute operations in the information environment. We will keep the committee regularly informed on our progress.

(U) Within DoD, we view our efforts to combat disinformation, misinformation, and propaganda in four broad lines of effort all supported by a foundation of intelligence support, interagency collaboration, and partnerships: 1) countering propaganda by adversaries, 2) force protection, 3) countering disinformation and strategic deception abroad by adversaries; and 4) deterring and disrupting adversarial malign influence capabilities.

(U) Countering Propaganda

(U) Propaganda, especially with a capable sponsor spreading it to susceptible audiences, can often drown out truthful information and create barriers to fact-based messaging. Within DoD, Public Affairs is the lead for countering propaganda by adversaries that impacts U.S. military objectives and keeping domestic and foreign audiences informed of adversarial efforts to manipulate behavior in this domain. Other DoD capabilities support Public Affairs' efforts to lead proactively with truthful, verifiable, fact-based messaging. DoD efforts to engage foreign

audiences overseas support the leading U.S. Government role played by the Department of State to inform and influence foreign audiences.

(U) Force Protection

(U) Our Soldiers, Sailors, Marines, Airmen, Guardians, civilians, and their families are part of the American public directly targeted by malign actors' disinformation, misinformation, and propaganda. DoD views this as a critical force protection issue. The Services are proactively leading efforts to enable resilience against these threats. Enabling the force to recognize deceptive information tactics by adversarial information operations, developing digital literacy, and employing critical thinking skills are a few key initiatives within this line of effort.

(U) Countering Disinformation Abroad

(U) DoD also possesses operational and informational capabilities, such as Military Information Support Operations (MISO), to generate narratives to compete against disinformation efforts directed at foreign audiences. These DoD capabilities can amplify as well as act in a complementary manner to inform audiences that cannot be reached through traditional communication channels. We will take a comprehensive and deliberate approach in consultation with the Department of State, taking into account the agility, capability, and capacity to connect with audiences globally in real time to build communications that foreign audiences trust. Knowledge and trust by foreign audiences will reduce and even suppress the impact of malign influence activities. DoD will continue to review ongoing work within the Department of State and seek ways to increase collaboration with the Department of State to optimize such efforts against these evolving threats and challenges in the information environment.

(U) Deterring and Disrupting Adversarial Malign Influence Capabilities

DoD's greatest strength lies in its capability to align narratives, actions in the land, sea, air, cyber, and space domains, and information-related capabilities against key weaknesses in the adversaries' information environment. Additionally, DoD has the knowledge, skills, and

infrastructure to enable partners, allies, proxies, and surrogates to compete with malign actions as peer competitors in the information environment. DoD's ability to execute Dynamic Force Employment enables diplomatic actions to deter malign behaviors by adversaries, incentivize their cooperation, or, when necessary, compel action.

(U) In addition to DoD's ability to match words with deeds, we also complement these actions with ongoing efforts to defend forward, which actively detects, assesses, and, when directed, disrupts adversaries' disinformation, misinformation and propaganda.

(U) Pursuant to section 1239 of the NDAA for FY 2020, we also are working to develop the comprehensive strategy to counter the threat of malign influence by the People's Republic of China and the Russian Federation. Those efforts are developed in concert with interagency partners, coordinated by the National Security Council staff.

(U) Partnerships and Intelligence Support

(U) Underpinning all these efforts is a strong commitment to a whole-of-government partnership and decision cycle that constantly assesses the effects of misinformation and propaganda, and seeks to attribute those efforts to the responsible parties. This requires active cooperation across responsible departments and agencies as well as direct support from the Intelligence Community. DoD leverages its information capabilities to gain and maintain the information advantage and integrates with the tools of other departments and agencies as part of a broader and more comprehensive approach. Our international allies and partners also bring reinforcing and often unique capabilities to countering adversaries' malign efforts; their capabilities will be integrated into our planning efforts as well.

(U) The recently signed Defense Intelligence Strategy (DIS) prioritizes the threat from China and Russia. The strategy calls out the specific action to prioritize intelligence support to strategic competition and influence efforts. The Defense Intelligence Enterprise (DIE) will help advance U.S. influence and counter coercive campaigns via intelligence support to sensitive and special activities, influence, deception, and operations in the information environment. We would like to

highlight for the committee three specific examples of ongoing actions that the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) is supporting by leveraging its roles within DoD and the greater Intelligence Community: 1) Intelligence support to Irregular Warfare, 2) Intelligence support to Operations in the Information Environment (OIE), and 3) Intelligence dissemination to support Combatant Command Messaging.

(U) Intelligence Support to Irregular Warfare

(U) In support of the Irregular Warfare (IW) Annex to the 2018 National Defense Strategy, OUSD(I&S), in partnership with the Joint Staff J2, supports specific lines of effort to enable DoD to improve understanding in a Multi-Domain Environment. The several lines of efforts focus on identifying Indicators and Warning, integrating collection, leveraging big data, reinforcing intelligence-sharing best practices, and assessing policies and processes to support these efforts.

(U) Intelligence Support to OIE

(U) In December 2018, the DoD Information Operations Executive Steering Group (IO ESG) directed the formation of a working group to optimize intelligence support to OIE. In April 2019, OUSD(I&S) chartered the Defense Intelligence Support to Operations in the Information Environment Working Group (DISOIE-WG), whose members include representatives from across OUSD(I&S), the Office of the Under Secretary of Defense for Policy, the Office of the Under Secretary of Defense for Acquisition and Sustainment, the Combat Support Agencies, the Defense Counterintelligence and Security Agency, the Joint Staff, the Joint Information Operations Warfare Center, and Intelligence representatives from each of the Services and U.S. Special Operations Command. The DISOIE-WG was created to improve intelligence integration and support to OIE by examining how collection, analysis, and prioritization of intelligence activities and capabilities can be optimized through policy, oversight, governance, enablement, and advocacy.

(U) In 2020, the DISOIE-WG proposed a new effort to focus National Intelligence Community collection efforts on assisting the conduct of influence-related activities against key adversaries. That work is still ongoing.[1]

(U) Currently, the DISOIE-WG is focused on drafting and staffing a new DoD Instruction for intelligence support to OIE activities; acting upon recommendations in a 2019 Joint Review Oversight Council Memorandum on OIE to address the Joint Staff capabilities based assessment; directing the DIE to prioritize resources for intelligence support to OIE in the next published Consolidated Intelligence Guidance; and engaging and participating in the National Intelligence focus groups to help drive key concepts related to OIE activities.

(U) Combatant Command Support

(U) Another line of effort for which DoD is providing intelligence support to OIE has been the joint DoD-Director of National Intelligence (DNI) response to the intelligence demands from the Combatant Commands. In January 2020, nine Combatant Commanders signed a memorandum, known colloquially as the "36-star memo," asking for increased support from the Intelligence Community for messaging and countering disinformation operations as part of great power competition. In response, the USD(I&S) and DNI partnered in an ongoing effort to streamline processes for downgrading, declassifying, and disclosing intelligence in support of OIE. DoD will look to complete the current efforts in response to the "36-star memo" by September 2021, while continuing with follow-on initiatives to increase the use of Open-Source intelligence and to determine policy and resourcing strategies to provide the most effective intelligence support to OIE going forward. Additionally, DoD is working to improve its training of intelligence personnel and to optimize its tradecraft as appropriate to support OIE.

(U) In conclusion, DoD recognizes the threat of disinformation, misinformation, and propaganda; we continue to invest our capability to improve employment of information operations and other tools to mitigate and defeat our adversaries' disinformation efforts. We will

[1] (U) COVID-19 impacted the Working Group's 2020 objectives.

continue to improve our speed, agility, efficiency, teamwork and most importantly – effectiveness.