COUNTERING THE "INFORMATION CONFRONTATION" STRATEGIES OF RUSSIA AND CHINA

Workshop Summary

September 27-28, 2022

Center for Global Security Research
LAWRENCE LIVERMORE NATIONAL LABORATORY

Workshop Summary

COUNTERING THE "INFORMATION CONFRONTATION" STRATEGIES OF RUSSIA AND CHINA

Center for Global Security Research
Livermore, California, September 27-28, 2022

Prepared by Lesley Kucharski, Mike Albertson, Marimar Calisto, and Brian Radzinsky[1]

On September 27-28, 2022, the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory (LLNL) hosted a workship titled "Countering the 'Information Confrontation' Strategies of Russia and China." The workshop explored how Russia and China use information as a domain of conflict in the 21st century, focusing on cognitive and psychological effects of information operations. It also took stock of US and allied responses to this challenge and explored what the allied community can, should, and should not do moving forward.

CGSR chose the term "information confrontation" as the organizing concept for the workshop for several reasons. First, information confrontation is a defined concept in the Russian strategic lexicon that evolved from Soviet military thought. According to the Defense Intelligence Agency, "'Information confrontation,' or IPb (informatsionnoye protivoborstvo) is the Russian government's term for conflict in the information sphere. IPb includes diplomatic, economic, military, political, cultural, social, and religious information arenas, and encompasses two measures for influence: informational-technical effect and informational-psychological effect. Informational-technical effect is roughly analogous to computer network operations, including computer-network defense, attack, and exploitation. Informational-psychological effect refers to attempts to change people's behavior or beliefs in favor of Russian governmental objectives. IPb is designed to shape perceptions and manipulate the behavior of target audiences. Information countermeasures are activities taken in advance of an event that could be either offensive (such as activities to discredit the key communicator) or defensive (such as measures to secure Internet websites) designed to prevent an attack."[2]

Second, the US strategic lexicon lacks a term that encompasses the entire scope of the challenge posed by Russia and China. In contrast to other domains of conflict, the United States does not weaponize information. Information confrontation is therefore an asymmetric challenge for the United States and its allies. Finally, information confrontation is deeply embedded in China's strategy, although China does not use the same term, and it has its own distinct ways of advancing its narrative priorities.

[1] The views and opinions of author expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

[2] 2017 Russia Military Power Report, Defense Intelligence Agency, p. 38, https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/Russia_Military_Power_Report_2017.pdf

The discussion was guided by three key questions:

- How have US adversaries conceived and conducted "information confrontation" across the continuum of conflict?
- How have the US and its allies responded?
- What more can and should be done to more effectively counter Russian and Chinese strategies?

Key take-aways:

- Russia and China are not a monolithic threat in the information space. There are significant similarities and differences in Russian and Chinese information confrontation strategies. Their strategic ends overlap to the extent that both Moscow and Beijing prefer a multipolar world order in which US influence is greatly diminished. Both seek increased influence vis-à-vis the United States, particularly in ther primary regional security environments. Yet, Russia aggressively seeks to divide and destroy US alliances and partnerships, while China places more emphasis on supplanting those structures with alternative structures, consistent with its long-term perspective. Whereas the Russian model for ways and means is narrative-centric, the Chinese model is platform-centric. Russia primarily floods information platforms with disinformation and tailored narratives, while China seeks to co-opt information platforms, including traditional and social media companies, think tanks, academia, businesses, and international diplomatic fora. China's platform-centric model lays a stable foundation for promoting disinformation and tailored narratives.

- The war in Ukraine thus far illustrates the limits of Russian and Chinese information confrontation. The success Russia had in shaping local, regional, and global perspectives about its illegal annexation of Crimea in 2014 was not repeated in 2022. Chinese information confrontation about Ukraine has been limited to opportunistic amplification of certain Russian disinformation and narratives. Russia has thus far failed to shape local and regional perspectives beyond Russian-speaking audiences in Russia and occupied areas of Ukraine. In contrast, Ukraine has successfully leveraged the information environment locally in most of Ukraine and regionally across NATO and the EU. The United States played a key role in this process by leveraging its Intelligence Community (IC) to pre-bunk Russian narratives about the invasion. Russia and China have experienced mixed success in shaping global perspectives about the war in Ukraine. Their successes include shaping narratives around food and energy security in Africa and the Middle East, as well as narratives about the transition to a multipolar world order in which Russia and China have more influence through organizations like the Shanghai Cooperation Organization and BRICS. However, the US and its allies have begun to prioritize countering these narratives, including by leveraging the United Nations General Assembly (UNGA).

- In the post-2014 security environment, the US government (USG) response to Russian and Chinese information confrontation has been largely reactive, ad-hoc, and focused disproportionately on countering specific narratives, leaving the private sector to address challenges related to controlling the platforms used to spread disinformation and propaganda. The USG made important strides with its successful pre-bunking of Russia's invasion of Ukraine in 2022, although it is unclear whether the war in Ukraine will be a watershed for US counter-information confrontation strategy. This strategic adaptation process faces three key challenges. One is the lack of timely, decisive interagency actions due to the wide-ranging scope of the challenge. A second is balancing public and private sector interests that come into conflict, including first amendment rights and the financial incentives of social media platforms. A third challenge is the lack of agreed metrics for assessing the effects of Russian and Chinese information confrontation as well as the effects of US countermeasures.

- As the US continues to adapt its approach, it can learn lessons from the range of strategies pursued by its allies and partners. Russia's information operations in Crimea in 2014 led EU and NATO countries to develop a proactive posture that focuses on tracking and exposing Russian disinformation. After Russia's full-scale invasion of Ukraine in 2022, the EU adopted more aggressive countermeasures, including blocking Russian media outlets Sputnik and RT. While NATO has been slower to engage this space than the EU, it produces high-quality threat analysis at the NATO Strategic Communications Center of Excellence (StratCom COE) in Riga. Similar coordinating mechanisms are not present among US allies in the Indo-Pacific region.

- Moving forward, the United States should develop a more proactive approach by enhancing resiliency against false narratives and projecting truthful American narratives. Aspects of the United States Information Agency (USIA) established during the Cold War provide insights for a modern "Information Operations Dojo." The current challenge requires extensive collaboration between the USG and the private sector, which owns the platforms and produces creative content.

Panel 1: Russia's Approach to Information Confrontation

- What are the main elements of Russia's approach?
- Does it conceive different roles in peacetime, crisis, and war?
- How does it assess its competitive position vis-à-vis the US and its allies?
- Has its approach evolved over the last decade? Why? Why not?

Participants generally agreed that the primary goal of Russia's information confrontation strategy is to maintain the Kremlin's information security while degrading the information security of external and domestic actors who are opposed to the Kremlin. The Kremlin seeks to establish a permissive environment for operational latitude while escaping consequences for its actions. This strategy is rooted in the Soviet theory of reflexive control, which seeks to influence adversary decision-making. Russian strategy is tied to regime legitimacy and security. The Kremlin uses propagandists to generate and sustain a sense of existential threat by spreading narratives about impending conflict with the West, primarily NATO and the United States. This existential threat is used to justify Putin's ambitions and the Kremlin's policies both internally and externally.

Participants debated whether Russia aims to degrade truth and sow chaos or to promote its own alternative truth, suggesting that the Russian approach is probably context-dependent. Some participants argued that the Kremlin is not necessarily concerned about convincing everyone of the truth of its narratives because the goal of these continuously repeated narratives is to establish a state of "anesthetized apathy" among targeted populations regarding the Kremlin's actions and policy influence over targeted decisionmakers. The firehose of Russian WMD-themed disinformation in the Ukraine conflict, particularly regarding alleged US BW laboratories in Ukraine, can be seen through this lens. Others argued that the Kremlin is interested in convincing others of the truth of certain narratives, particularly those related to strategic stability and the future world order. For example, Russian narratives about the perceived dangers of NATO nuclear-sharing arrangements and NATO expansion are historically consistent. Moreover, since at least the 2007 Munich Security Conference, Putin has promoted his vision of a multipolar world order in which the United States is no longer the perceived global hegemon.

The discussion highlighted that Russia utilizes a mix of old and new tools and tactics to achieve its information confrontation objectives. Tested tools and tactics from the Soviet era include spreading disinformation through diplomatic platforms and traditional media, covert political funding, the use of NGOs, and influencing selected academic experts. New tools include information laundering and "information sovereignty," while new tactics include the use of global social media platforms. Some participants cautioned against focusing too much on Russia's use of social media, noting that disinformation dissemination through traditional media tools is still effective. For example, Russia propagates WMD disinformation about the Ukraine conflict through traditional diplomatic channels, newspapers, television, and social media, particularly Telegram.

Workshop participants agreed that Russia does not share Western conceptions of the continuum of conflict. It understands peacetime, crisis, and war as fluid states rather than as discrete steps. Russia constantly changes the thresholds between these states in response to what it perceives an adversary is willing to accept. The least intense manifestation of Russian information confrontation involves propaganda quietly disinforming, demoralizing, and destabilizing adversary audiences to replace truth with Moscow's preferred reality. When Russia perceives its political, social, and cultural norms are under threat, it activates mass media to influence audiences. For example, Russian state media used the 1999 apartment bombing in Moscow to shape perceptions in favor of the Chechen War. In war, the Kremlin closes independent media, blocks opposition social networks, implements draconian laws against protests, and heavily proliferates disinformation, as seen during the "Special Military Operation" in Ukraine.

Russia assesses its position vis-à-vis the US and its allies as competitive. Participants emphasized that Moscow fundamentally rejects Western values that underpin the world order because it perceives them as double standards through which the West, particularly the United States, acts with impunity as the global hegemon. Instead, Moscow offers a vision of a multipolar world order in which Russian, Chinese, and other national values have more global influence. Nikolai Patrushev, head of the Russian National Security Council, describes Russian values as "equality, justice, non-interference, and national sovereignty." Moscow believes it should protect Russia and like-minded countries from what it perceives as threatening neoliberal trends of individualism, egoism, consumerism, and self-expression. To convince external and domestic audiences that the Kremlin is acting correctly while adversaries are at fault for starting crises and wars, the Kremlin creates myths about the persecution of ethnic Russians, including spreading lies about human rights violations. This way, Russian authorities can disguise their aggression as humanitarian action and effectively demonize adversaries. It remains to be seen whether Russia's informational performance in Ukraine since February 2022 results in a strategic failure and the erosion of its relationships with the international community beyond the United States and its allies.

Recalling Soviet "active measures" during the Soviet invasion of Afghanistan, participants noted that the Russian approach is rooted in the Cold War and has evolved significantly over the years. Participants stressed that the Crimean operation was a turning point in how Russia assessed the effectiveness of information confrontation. Russia implemented lessons learned from previous conflicts and effectively used information confrontation to completely isolate Crimea from the regional and global information environment. This isolation allowed Russia to achieve a quick and nearly bloodless fait accompli. Yet participants debated whether Russia's invasion of Ukraine in 2022 demonstrates that information confrontation is now relegated to a supportive role while conventional warfare and nuclear deterrence of NATO regained primary importance.

Panel 2: China's Approach to Information Confrontation

- What are the main elements of China's approach?
- Does it conceive different roles in peacetime, crisis, and war?
- How does it assess its competitive position vis-à-vis the US and its allies?
- Has its approach evolved over the last decade? Why? Why not?

According to the discussion, the primary goals of China's information confrontation strategy are to achieve "comprehensive modernity," accrue wealth, and displace what Beijing perceives as the US-led international system. Some participants drew parallels with the Russian approach, noting that China also aims to establish a new form of international relations without the perceived liberal bias of the rules-based international order imbued in forums like the United Nations. Yet others made contrasts, arguing that China has the ways and means to achieve its vision of world order.

When discussing the ways and means of China's strategy, participants noted that China's approach is platform-centric, reflecting the Chinese Communist Party's (CCP) perceptions about politics and power. In order to control the marketplace of ideas, the CCP seeks to control information dissemination platforms across societies. By controlling who gets a voice in politics, academia, entertainment, and the media, the CCP promotes preferred messages while censoring anti-CCP content. Controlling platforms also allows China to promote specific narratives that legitimize the CCP and communist control as an alternative to liberal democracy. This approach traces back to Mao Zedong, who said that the United Front and armed conflict are the two basic weapons in the hands of the CCP to defeat its enemies. Xi Jinping uses this framework to "rejuvenate" China through, among other policies, a major modernization of the United Front and the People's Liberation Army (PLA).

The CCP seeks to mobilize the entire Chinese nation through United Front work, which is woven into all aspects of Chinese administration. Each ministry contributes to the United Front. For example, the Ministry of Education sets up Confucius Institutes for international exchanges and outreach to external academic institutions. The United Front pursues lines of effort to control the ethnically Chinese diaspora worldwide, facilitate technology transfer to China, and co-opt international elites to work for the CCP. These efforts also carve a path for Chinese intelligence services.

Like Russia, China has a fluid conception of the continuum of conflict. The CCP defines security as the absence of threats to the regime, which suggests that the CCP is in a constant search for enemies. CCP leadership perceives itself as in a crisis or conflict state with the United States because it views US values like the rule of law and constitutionalism as threatening. The line between offensive and defensive measures is blurry in the Chinese information context because China defends against what it perceives as dangerous ideas by preemptively censoring or guiding conversations. For this reason, there is no independent Chinese media. One participant noted that the CCP also owns or influences around 80% of media in Taiwan. The CCP's tactics change when it deems that subtle influence is unsuccessful. Some participants argued that the CCP's ambitions toward peaceful reunification with Taiwan are approaching this point. If the CCP can no longer envision a positive outcome with influence alone, it is likely that it will take more overt and destructive measures to achieve its ends.

The CCP views its position as competitive vis-à-vis the US and its allies. Particpants discussed how this confidence stems in part from the CCP's belief that it has successfully framed the global debate on China, including by weaponizing race sensitivities. The CCP also successfully wields China's powerful market to influence adversary nations. One participant highlighted the CCP's policies in rare earth metal processing as an example. To prevent any other nation from becoming an alternative to China for green energy, which relies on certain rare earth metals, the CPP establishes joint ventures with companies that mine rare earth metals. If a company seeks to develop its own processing capabilities, it is threatened by its CCP-backed joint venture partner. Some participants noted the CCP has also developed inroads in international forums to achieve these and other ends.

Panel 3: Case Study: The Ukraine War

- Has Russia's strategy worked well for it? Has China's?
- Has either modified its approach in light of lessons learned?

- Have the US and its allies been effective in countering their strategies?
- What lessons should they learn?

From the lead up to the invasion and throughout the war, Russia has employed a wide variety of false narratives to defend and obfuscate its war in Ukraine. This includes not only disinformation, but the active manipulation of the information environment using multiple sources. Many of these false or misleading narratives build on longstanding Soviet WMD narratives, such as the Soviet disinformation campaign claiming that the United States created the virus that causes AIDS. Russia seeks to capitalize on the widespread public fear that WMD generates. Russia used false claims about WMD in Ukraine to justify its "Special Military Operation" in Ukraine, and some participants argued that Russia could use these claims to justify its own potential use of WMD in the conflict. Russian information confrontation in the Ukraine war has been very opportunistic, although participants noted that it is often unclear whether Russia is strategically sowing the seeds for future exploitation or is simply looking for tactical successes against the backdrop of setbacks in its conventional warfighting campaign. The sheer mass of Russian disinformation alone generates some opportunities for success around the globe.

Participants noted that the CCP opportunistically amplifies certain Russian narratives and disinformation about the Ukraine conflict. For example, the CCP amplifies Russian narratives about NATO and the US being at fault for the conflict. The CCP also amplies Russian narratives about alleged US BW laboraties in Ukraine and in other countries. Some participants argued that the CCP amplifies Russian BW narratives to deflect conspiracies about the origins of Covid-19.

Participants varied in their assessments of Russian information confrontation in the Ukraine war. Many argued that key aspects of Russia's campaign have failed. For example, attempts to justify the invasion by depicting the Ukrainian regime as Nazis with WMD failed to gain traction in the West. The Kremlin lost the information initiative in the first month and has thus far failed to regain it. Participants noted that the Kremlin's attempts at disinformation have been at times unsophisticated, as seen in the failed deepfake of President Zelensky. Russian political leadership apparently began to believe their own lies about Ukraine, and the Kremlin likely overestimated its ability to win in the information space like it did in Crimea in 2014. The information domain became one in which private and public actors are actively supporting Ukraine, making this a hostile and competitive environment for Russia.

Failure of the disinformation campaign in the West can be linked to two main factors, according to several participants. First, the Ukrainians have been superb in flooding the information space with their own emotionally-resonant content, including memes and jokes about Russian ineffectiveness. The Ukrainian effort has been largely grassroots, the product of a broader national mobilization, and thus can be more agile and risk-acceptant than an official government campaign. Second, the United States and its allies demonstrated some progress in their counter-disinformation education and practice. They focused on intelligence and information sharing, public and private partnerships, and strategic messaging to preemptively pre-bunk or quickly de-bunk Russian disinformation.

Others argued that the record on Russian information confrontation in the Ukraine war is mixed. Moscow's efforts are effective in the tightly controlled Russian information space, although cracks in that foundation are starting to emerge with continued military failures and the partial mobilization campaign. Moscow's narratives and disinformation are also working in pockets within Ukraine, particularly in the occupied regions. Participants noted that this success is due in part to Telegram, which several participants described as the central platform for information confrontation in the Ukraine war. Moscow has also seen some successes in targeting the Middle East and Africa with messages about food and energy security. Multiple participants warned that some Russian and Chinese disinformation about the war is gaining traction in the West, noting that public opinion polls and discussions in fringe communities like QAnon suggest that disinformation about alleged US BW laboratories in Ukraine is a case in point. Others noted that Russia continues to raise the issue of US compliance with the BWC at the UN, and that many countries, including China, are not countering this effort. Some participants further argued that Russian efforts to target war fatigue among countries supporting Ukraine may also yield success for Moscow.

Participants identified lessons the US and its allies can take moving forward in their efforts to counter Russian and Chinese information confrontation in the Ukraine conflict. In general, participants stressed that the US and its allies must recognize that Russia will continue targeting audiences in both the West and the rest of the world as the war continues in an attempt to promote Russian strategic narratives while sowing divisions and doubt about the objective truth on the ground in Ukraine. In particular, the US and its allies should strive to respond at the speed of relevance by improving narrative tracking, response coordination, and dissemination of strategic and public communications. While they were successful in pre-bunking Russia's narratives around its February 2022 invasion, the West has yet to gain the initiative in countering certain narratives, particularly surrounding Russian BW allegations.

Russia is undoubtedy learning lessons from its successes and failures in the Ukraine war and weaving them into its future plans. Whether this includes doubling down on past practices to exert more control over Russia's domestic information ecosystem, crafting new narratives and disinformation to manipulate perceptions of the war domestically and abroad, or other methods remains to be seen. Participants cautioned that the interwar Russian capacity for adaptation should not be dismissed.

Panel 4: Calibrating the Challenge to the US and its Alies

- What are the main features of the challenge we now face?
- What are the differences between disinformation and deterrence signaling?
- What are the differences between disinformation and competition in the cognitive domain?

To calibrate the information confrontation challenge to the US and its allies, participants discussed the importance of recognizing the differences in Chinese and Russian replacement narratives. China seeks to replace the existing global order with a Sino-centric order, where countries accept China as the preponderant global power. Thus, its replacement narrative is centered on co-optation of existing platforms and institutions. Some participants argued that the successful advancement of this replacement narrative requires tearing down the US-led post-WWII system and selling the alternative narrative of a China-based system as inevitable.

In contrast, participants noted that Russia's replacement narrative is more complex. It is tailored to both domestic and international audiences. Domestically, the Kremlin seeks to counter the

Western-leaning neoliberal narrative with a neo-Tsarist Russian Orthodox narrative that is based on historical grievances and glories, as well as loyalty to the motherland and the regime. Russian propagandists sow fear of liberal values that they say are destroying “traditional” alliegences to family, church, and state. Moscow’s external replacement narrative emphasizes the role of Russia in catalyzing a shift towards a multipolar world in which Russia has more influence, and US hard and soft power is greatly diminished. Russia does not claim the right to dominate the world system, but it does desire more influence over its regional security environment. Participants noted that Putin’s 2007 Munich Security Conference speech represented a turning point for Russia’s replacement narrative against NATO. The renewed effort incudes a revisionist vision of history and arms control, a mythology concerning the alleged dangers of NATO enlargement, and the targeting of specific policies that are divisive in the alliance, such as nuclear deterrence and the presence of US nuclear weapons in Europe.

Because of these fundamental differences, the US and its allies must tailor their counterstrategies to Chinese and Russian information confrontation. Participants debated the merits of pitting the Western notion of democratic truth against the authoritarian truths promoted by the CPP and the Kremlin. Some proposed that the West build upon successful experience from the Cold War by highlighting where the West succeeds and the adversary falls short. Yet others argued against this approach, emphasizing that pitting one truth against a contending truth legitimizies the problematic notion that there are multiple truths. This approach is particularly problematic with disinformation about alleged US BW laboratories in Ukraine and other countries. Participants further noted that many countries do not want to take sides in a zero-sum debate, as in the Cold War.

In tailoring counterstrategy to China, participants suggested that the US and its allies emphasize the moral imperative to protect sovereign peoples from domination by a Chinese tributary state system. Some participants stressed that the West seek to deflate CCP statements about how it governs China, highlighting human rights abuses as well as CCP corruption, incompetence, and infighting.

Participants stressed that tailoring counterstrategy to Russia requires recognizing that the current reactive “whack-a-mole” approach to countering the Kremlin’s disinformation and misleading narratives is neither effective nor sustainable. For example, some participants highlighted that NATO is still playing catch-up with Russia over narratives related to the effects of the Ukraine war on global food security, particularly in Africa. One participant stressed that the Russian replacement narrative is harder to fight because the Kremlin is targeting perceived weak points in the international rules-based order, including the absence of a verification mechanism within the BWC and disagreements within NATO about how the alliance should respond to attacks against partners, who are not protected by Article 5 of the North Atlantic Treaty. Other participants highlighted that the Kremlin is exploiting the West’s own internal political divisions. Countering this aspect of the challenge requires the West to mitigate domestic polarization.

Calibrating the challenge also requires some degree of perspective. One participant cautioned against conflating adversary deterrence signalling and disinformation. Bluffing, blustering, and nuclear sabre-rattling are part of standard deterrence practice and should not be described as disinformation. Describing deterrence signalling as disinformation may lead Moscow to pursue potentially more escalatory steps to communicate stake and resolve. This participant further argued that the narratives promoted by Russia and China about the dangers of US alliances likely reflect sincere threat perceptions. Russia, for example, has identified NATO nuclear-sharing arrangements and the expansion of NATO as threats for decades. Describing these threat perceptions as false instead of recognizing them likely reinforces the Kremlin's threat perceptions and may increase the Kremlin's resolve to continue fighting against what it describes as a US- and NATO-backed puppet regime in Ukraine. Rather than deny Russia and China their threat perceptions, the US and its allies should pursue other military and non-military ways and means to influence their strategic calculus.

The same participant also cautioned against conflating competition in the information domain and disinformation. Describing all Russian and Chinese narratives as disinformation and dismissing the need to engage them is not always a competitive strategy. For example, global reactions to the war in Ukraine demonstrate that Russian and Chinese grand strategic narratives about the transition away from US global hegemony to a multipolar world order are resonating in non-aligned areas of the world, particularly those with colonial legacies. Further, discussions within the UN about alleged US BW laboratories in Ukraine and in other countries bordering Russia and China suggest that naming and shaming Russia and China for their promotion of this disinformation without providing timely or substantive counternarratives does not appear to be competitive outside US alliance structures and even within certain Western communities, including QAnon.

Panel 5: Taking Stock of US Responses

- Looking back over the past decade or so, how has the US responded to this emerging challenge?
- Has its approach evolved? Has it learned the right lessons from its experience?
- Has it been effective? If so, why? If not, why not?

Recalling Soviet disinformation and other "active measures" during the Cold War, participants emphasized that this challenge is not new. The USG has historically responded to this challenge as it evolved. During the Cold War, the USG established the USIA to counter Soviet and other global information challenges. After the collapse of the Soviet Union, the USG disbanded the USIA and transferred some authorities to the Department of State (DOS). In the post-9/11 security environment, DOS established the Global Engagement Center (GEC) to coordinate interagency communications and counter disinformation from foreign state and non-state actors. Participants noted that the USG response to this challenge over the past decade or so can be characterized as a period of transition in response to the re-emergence of major power rivalry, particularly after Russia illegally annexed Crimea in 2014 and interefered in the 2016 US Presidential election. The 2017 National Defense Authorization Act expanded the GEC's mandate to focus on state actors—especially Russia, China, and Iran—involved in manipulating the global information space using tools such as algorithms, fake sites, and bots to disseminate and amplify disinformation and specific narratives.

Some participants described the USG's current approach to responding to the major power rivalry aspect of the information threat as "building the plane as we fly it," suggesting that the USG recognizes the need to adapt to the evolving threat at the speed of relevance but that the record on learning the right lessons is mixed. On the positive side of the ledger, participants noted that the GEC's approach reflects important lessons from public opinion polls and studies in psychology indicating that attempts to directly de-bunk every lie, half-truth, or misrepresentation can add credibility to disinformation while doing little to change minds. Instead, the GEC aims to expose the networks of foreign state actors that manipulate the global information space. To achieve these ends, the GEC coordinates with the US interagency and cooperates with the private sector, which controls the information platforms and produces creative content. For example, the GEC successfully leveraged these connections to pre-bunk Russia's invasion of Ukraine in 2022.

The record on enhancing USG cooperation with the private sector is mixed. Participants described the USG's relationship with the private sector as limited to regular consultation. This limited relationship stems from the unique constraints of the US Constitution and a preference for self-regulation among US-based social and traditional media companies. A lesson to be learned from these structural constraints is that the USG would benefit from trust and confidence building measures with the private sector in the information space. Participants agreed that the USG is making progress towards this end, noting that the relationship has deepened over time, especially after the 2016, when Russia exploited social media companies to interfere with the US Presidential elections. In general, cooperation between social media companies and the USG is facilitated by the fact that both actors pursue relatively similar strategies for countering information confrontation. For instance, Facebook parent-company Meta's model for countering "coordinated inauthentic behavior" on its platforms also involves exposing networks of malign content producers and disseminators. Further, neither actor has opted to position itself as an arbiter of truth. Yet participants also stressed that more can be done to enhance this relationship. Participants identified foreign language and cultural competencies as a promising avenue for cooperation in countering information confrontation efforts. One participant stressed that such cooperation would have helped the GEC respond to genocidal language circulating in Ethiopian social media during the Ethiopian civil war. This participant explained that both the GEC and social media companies lacked personnel fluent in Amharic and other local languages.

On the negative side of the ledger, attempts to coordinate USG responses in a centralized manner, as was done during the Cold War through the USIA, have thus far failed. In this regard, participants noted the stalled deliberations within the National Security Council (NSC) as well as the quick rise and fall of the Department of Homeland Security (DHS) Disinformation Governance Board in 2022. Yet, some participants cautioned against drawing the wrong lessons from past experience. For example, instead of seeking to emulate the centralized approach of the USIA in the contemporary information environment, the USG should draw inspiration from the way the USIA incorporated Madison Avenue advertising and branding expertise to project positive images of American society.

Panel 6: Taking Stock of Allied Responses

- Looking back over the past decade or so, how have US allies in Europe and Asia responded to this emerging challenge? Have their approaches evolved?
- Have they been effective? If so, why? If not, why not?
- What lessons should the US learn from their successes and failures?

Allied responses to information confrontation differ between Europe and Asia. In Europe, participants agreed that the NATO alliance as a whole, as well as individual members, have recognized and adapted to the threat from Russia. In 2014, NATO created the StratCom COE to better understand and track disinformation threats and serve as the alliance's principal response entity for disinformation. The StratCom COE tracked Russia's massive, automated content generation campaign that preceded the invasion of Crimea in 2014 and coordinated NATO's response. While a growing body of evidence that Russian military and intelligence personnel were largely surprised by Russia's "Special Military Operation" in 2022 suggests that Russia was not prepared to deploy a globally effective information campaign as it did in 2014, the StratCome COE continues to find that Russia remains a capable actor in the information domain.

Despite the StratCom COE's competence and importance to NATO efforts, participants noted that its products are not widely used within NATO HQ or by the EU and other regional institutions. With respect to NATO HQ, it is unclear whether this reflects poor demand, a lack of coordination, or both. Regarding the EU, it is unclear whether this reflects the COE's focus on NATO and, perhaps, a reluctance to reach outside of this focus. However, participants also generally acknowledged that the EU is ahead of NATO in countering information confrontation.

Asian countries are also recognizing a need to play an active role in the information sphere, although efforts vary widely across countries, and the "hub and spoke" nature of the US alliance framework in the region does not create ready mechanisms for coordination. The diversity of approaches is exemplified by the differing approaches of Australia, Japan, and India. Participants noted that the most forceful response of the three comes from Australia, which has passed laws enabling the government to play an active role in the information sphere. For example, foreign actors must register with the government before they are permitted to engage in the public sphere. Australia has also established a Foreign Interference Response Team and several other entities to manage different aspects of the information space, including a countering disinformation branch within the Department of Foreign Affairs and Trade, and a university foreign interference task force. The Homeland Defense Ministry and the Australian Election Commission also play roles in countering disinformation from both foreign and domestic actors.

A more recent approach comes from Japan. Japan is an important target of information confrontation, but particpants noted that the government has not yet seen a need to respond legally or bureaucratically. This may reflect the relative recent arrival of disinformation operations targeting the Japanese public. Until recently, disinformation regarding Japan primarily took the form of misrepresenting Japanese government positions and actions to third-party actors. For instance, Russian trolls have created fake news stories that purport to represent statements from Japanese government officials. Direct Russian targeting of the Japanese information space began after Tokyo adopted a version of the Magnitsky Act, which sanctions alleged human rights violators. China also began engaging in the Japanese information sphere, primarily to promote favorable views of China or to attempt to drive wedges between the US and Japan. The Japanese government has been slow to respond to this increase in disinformation, focusing primarily on de-bunking false information. Japanese media companies have adopted a different approach. Instead of directly de-bunking, they created a system that weighs official expert commentators more heavily in social media feeds and searches.

Participants described information confrontation as "rampant and severe" in India, but noted that the government has only recently engaged in countering it. Disinformation is one among several acute internal and external pressures on the Indian information environment, which is also pervaded by a competitive media experiencing “tabloidization,” significant ethnic tensions that increase vulnerability to disinformation, and a related threat from violent extremist organizations, particularly those operating from Pakistan. Participants highlighted that the information dimension of the Doklam border crisis with China in 2017 was a wake-up call for the Indian government. Since then, the Prime Minister leads many messaging efforts. The government response is largely driven by individuals rather than institutions.

US and allied experience offer both lessons and warnings for all parties. One clear lesson from the Australian case is that governments can only act as aggressively as their laws and institutions will permit. The question for countering information confrontation is whether there are additional opportunities to take advantage of legal mechanisms in those states where legal remedies are possible. In more institutionally constrained environments, there may instead be lessons to be learned in sharing tactics, techniques, and procedures for coordination of government responses, declassification of necessary information, and dissemination of responses. Allies can also provide the US with area-specific knowledge that can help refine ongoing efforts, such as those led by the DOS GEC. In Asia, for instance, small newsroom staffs mean that GEC efforts to train journalists can come at a significant cost for some publications. Allies can help find ways to better reach key actors who may be reluctant to engage with government actors for prudential reasons.

Finally, participants stressed a need for the US and its allies to be more forward-leaning in advancing their own narratives in the information space. While the US and like-minded partners may be legally constrained and reluctant to go on the information offensive, there are opportunities to campaign for their values. For instance, in response to Russian efforts to discredit nuclear deterrence policies, allies could advance their own narratives of the role of nuclear deterrence in their foreign and security policies and promote these more aggressively in key forums.

Panel 7: Next Steps in Disarming Disinformation

- What should the US and its allies do to become more effective at countering false narratives?
- How can the information ecosystem be more effectively engaged? Are new institutions needed?
- What are the responsibilities of private sector actors?
- What expectations should we have about future effectiveness?

Disarming disinformation requires the US and its allies to expand their aperature beyond analyzing the challenge to synthesizing and implementing a counterstrategy that involves the public and private sectors in a whole-of-society approach. This counterstrategy must be tailored to the differences in Russian and Chinese information confrontation strategies. Participants identified four tenets of this approach. One tenet is balancing efforts to reactivley counter the Russian “firehose of falsehoods” with proactively developing and disseminating Western narratives. The pre-bunking utilized before Russia’s intervention in Ukraine is a successful model for further development. A second tenet is countering Chinese efforts to co-opt narrative dissemination platforms. The current approach to countering disinformation focuses primarily on countering the Russian narrative-centric model, leaving the Chinese platform-centric model largely unchecked. A third tenet is cultivating a culture of innovation that incentivizes risk-taking and testing different methods for countering disinformation and advancing our own narratives. A fourth tenet is developing resiliency through media literacy.

To more effectively engage the information ecosystem in countering disinformation at the tactical level, participants discussed how the US and allied governments can pursue multiple lines of effort:

1. Develop and proactively communicate their common story and narratives. The US and allied narrative is often reactive, underdeveloped, and drowned out by Russian and Chinese narratives. Developing counter narratives that are timely, tailored to Russian and Chinese strategies, and competitive within audiences across US alliances and partnerships is a challenge that does not lend itself to technical solutions. The US must avoid promoting narratives that are perceived as intrusive and culturally insensitive in allied and partner countries, but project positive messagage that reflect widely held Western values of democracy and freedom.

2. Empower authorities across the public and private sectors and provide a sustained budget for creative, collaborative content development. Otherwise, responses will continue to be reactive and ad-hoc. Given the cross-cutting nature of the challenge, the NSC is the natural center of gravity to coordinate this process in the United States.

3. Develop an "Information Operations Dojo" that operates on the open security concept used in computer security. Strategists and practitioners from the public and private sectors across the allied community can gather at the Dojo to teach and practice developing compelling content. They can also develop concepts for creating safe digital communities, drawing, for example, upon building codes for physical infrastructure. Recognizing that public disclosures increase resiliency (e.g. awareness around threat of deep fakes has thus far prevented their effectiveness), the Dojo could also provide a space to practice red-teaming disinformation operations.

4. Build upon the successful technology development efforts by the DOS GEC. The GEC Technology Engagement Team (TET) sponsors the creation of tools for countering disinformation across the supply-demand spectrum. Whereas supply-side products support content authentication, demand-side products support resilience through media literacy and sentiment monitoring. One successful use of sentiment monitoring products allowed the GEC to locate and concentrate engagement efforts on a hotspot in Africa where Russian BW disinformation was gaining traction.

5. Expand the platforms for promoting US and allied narratives. This involves moving beyond ephemeral social media content to movies, shows, and games that exert more long-term cultural influence. It should also involve changing the incentive structure for the private sector, which generally opposes heavy-handed regulation and no longer promotes positive messages about the United States at the level that was seen during WWII. The conflict in Ukraine provides lessons in government engagement with the private sector. Businesses willingly participate in sanctions against Russia, in contrast to their relative lack of response

to Russia's illegal annexation of Crimea in 2014, in part because the US and allied governments provided a clear and compelling rationale for doing so.

6. Improve media literacy. This effort should focus on the most vulnerable communities, such as the younger generations who have not been exposed to the type of public service messaging (e.g. Schoolhouse Rock!) that was common media literacy practice with older generations.

The private sector brings unique tools to bear in the fight against disinformation, although it also faces unique constraints. The power of the private sector stems from its control of the media platforms sustaining large portions of the information ecosystem across the United States, its allies, and other democratic countries. In contrast to the public sector, industry has fewer legal and normative constraints in shaping hearts and minds. Participants noted that there are a few small companies working in this space. Yet financial interests and company values often compete with civic responsibilities to counter disinformation. While Russian interference in the 2016 US Presidential election awoke social media platforms to their vulnerabilities to disinformation and other forms of information confrontation, companies take different approaches to the threat. While Meta exposes "coordinated inauthentic behavior," Twitter maintains a comparatively harder stance against regulation, although it has pursued effective measures such as account verification. Another aspect of this challenge is that the US and allied community has limited influence over popular social media platforms based in Russia and China, such as Telegram and TikTok.

Participants noted that the US and its allies must calibrate their expectations about future effectiveness. They should recognize that disinformation is a new persistent threat with no single solution. Countering this "new normal" therefore requires a layered approach. Recognizing resources constraints, the US and its allies should prioritize countering and protecting "critical narratives," drawing from the defense policy concept of "critical infrastructure." While some concepts from other domains are applicable to the information space, others are not. For example, participants stressed that many human vulnerabilities to disinformation cannot be patched with software or hardware updates. Finally, the US and its allies must recognize that this challenge requires efforts to resolve political polarization that is amplified rather than created by Russian and Chinese disinformation.

Panel 8: Next Steps in Countering Social and Political Manipulation

- What should the US and its allies do to become more effective at countering social and political narratives?
- How can the information ecosystem be more effectively engaged? Are new institutions needed?
- What are the responsibilities of private sector actors?
- What expectations should we have about future effectiveness?

As with countering disinformation, countering Russian and Chinese social and political manipulation requires a layered solution. Participants noted that this layered solution would benefit from a strategic framework that identifies central points of attack and categories of actors. In the information space, the three central points of attack are content origination, content dissemination and amplification, and content reception and impact. The three actor categories are civil society, media platforms, and governments. This layered scheme can guide the US and its allies in its efforts to influence the incentive structure for propaganda. For example, this scheme suggests that they should concentrate efforts on media platforms, which can develop pre-submission algorithms and modify their terms of service to encourage orginators and amplifiers to publish only verified information. To protect information receivers, they could provide warning stoplights that explain the credibility of the source and content. These stoplights can change over time to show how the content is being used.

Another layer of this solution is rethinking approaches to "soft power" in the 21st century information environment. One participant argued that the US and its allies should link soft power to defense and security through the framework of "reputational security," which recognizes positive and negative reputational effects as largely unacknowledged factors in past and current conflict. One successful historical example of reputational security is President Eisenhower's prioritization of domestic civil rights as a result of Soviet propaganda efforts to portray the US in a negative light globally over US racial divisions. Another example is the show "Space Bridges" hosted by Vladimir Pozner in the 1980s. One episode brought together ordinary citizens and nuclear scientists from the USSR and US to discuss nuclear safety in the wake of the accidents at Chernobyl and Three Mile Island. As the US and its allies draw inspiration from these historical examples, they should take care to not fulfill Russian and Chinese stereotypes about the West.

When seeking to engage the information ecosystem to counter social and political manipulation, some participants stressed that US and allied governments should work through existing institutions before creating new ones. Under the current US administration, political positions with relevant authorities remain unfilled. When reflecting on the history of the USIA, the US should recognize that the institution was not ideal. One participant remarked that its successes were often a result of Presidential buy-in or were won at high political cost, and it also experienced many failures. Yet participants also stressed that there are positive lessons to be learned from the USIA system of metrics for measuring effects on foreign audiences. The US can also look to its allies for positive examples of new institutions dedicated to countering social and political manipulation. Instead of following the Soviet and USIA models by which the government influences culture, the US can learn from the United Kingdom's British Council, which is a respected non-partisan cultural institution operating outside of government.

History provides lessons for private sector efforts to counter social and political manipulation. Participants noted that foundations historically played a large role in this space, with Hollywood being a special case. Walt Disney, for example, was at the forefront of countering foreign influence and promoting positive images of the United States. USG leadership historically plays an important role in influencing the private sector to take action. When the USG admits that a hostile country is behind social and political manipulation, private sector actors are empowered to take action.

As with countering disinformation, participants stressed the importance of calibrating expectations about countering social and political manipulation. Dramatic change is unrealistic and, in some cases, undesirable. The fate of the short-lived DHS Disinformation Governance Board illustrates how dramatic change often yields political controversy. In contrast, gradual change increases broad political support. This gradual approach should include an openess to negotiating with Russia and China in the information space, drawing from successful historical cases, such as the US response to Soviet disinformation about the US creating AIDS. The US successfully threatened to cut off scientific research collaboration if the Soviet Union did not stop promoting this false narrative. In the contemporary environment, the US and its allies could demand reciprocity from China in terms of access to media platforms, recognizing that this demand would be one layer of a long-term effort.

CGSR

Center for Global Security Research
Lawrence Livermore National Laboratory
P.O. Box 808, L-189 Livermore, California 94551
https://CGSR.llnl.gov

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.