THE COMING WAR IN AMERICA

The remarks below were delivered at a symposium on "The Coming War in America" hosted by the National Institute for Public Policy on January 20, 2026. The symposium assessed various irregular and often underappreciated threats to the United States posed by malicious foreign actors.

David J. Trachtenberg (moderator)
David J. Trachtenberg is Senior Scholar at the National Institute for Public Policy and previously served as Deputy Under Secretary of Defense for Policy.

Generals and other military officials have often been accused of planning to fight the *last* war, rather than the next, by failing to take into account the unconventional threats and non-traditional challenges that are generally unanticipated, yet are at least equally, if not more, serious and dangerous for U.S. security.

We are sometimes told that intelligence shortcomings that lead to unexpected and catastrophic events reflect a "failure of imagination" – in other words, an inability or unwillingness to look beyond traditional threats and familiar patterns of behavior that lead us to discount the possibility that adversaries may seek unusual, unexpected, and asymmetric means to threaten the United States.

Today's webinar focuses on various asymmetric threats and challenges that some may argue are too remote and unlikely to deserve serious consideration by policy makers, yet are often underappreciated in either their possibility or potential consequence.

Specifically, as I noted in the invitation to this event, today's discussion will focus on various scenarios for attacks on the U.S. homeland by a wide variety of nefarious actors, including nation-states Russia, China, Iran and North Korea, as well as various terrorist groups and transnational criminal organizations.

We will examine four plausible scenarios, including: 1) Adversary attempts to influence the outcome of the U.S. national elections in November 2028 through a campaign of targeted political violence and assassinations; 2) Adversary operations to disrupt the U.S. economy, including physical and cyber attacks on U.S. critical infrastructures; 3) Adversary attacks to degrade and delay U.S. munitions production and distribution; and 4) Adversary attacks to disrupt or degrade U.S. national decision making and strategic military operations.

Let me briefly comment on each of these scenarios in turn, before turning the floor over to the other panelists whose expertise in these matters is far greater than my own.

First, the prospect of adversary attempts to influence the outcome of the U.S. national elections in November 2028 through a campaign of targeted political violence and assassinations is not as far-fetched as some may prefer to believe. We have seen adversaries like Russia and China seek to sow political division within the United States whenever possible, using propaganda and downright disinformation. And we have also seen attempts to assassinate American politicians on U.S. soil because of their political views. Moreover, the

Department of Justice has documented multiple cases of foreign agents plotting assassinations in the United States.[1]

Currently, the nation is highly polarized politically and control of the legislative branch of government is up for grabs in this year's midterm elections. Republican majorities are slim in both the House and Senate. The balance of power could easily shift as a result of violence that swings political control from one party to another. This could also have implications for the 2028 presidential elections.

Second, the vulnerability of U.S. critical infrastructures to foreign sabotage that disrupts the U.S. economy is a growing concern. Back in 2014, an attack on an electric power station in California knocked out power around San Jose for nearly a month and raised concerns over a possible link to international terrorism.[2] Physical or cyber attacks that take down the energy grid, for example, can have cascading effects that degrade other critical national infrastructures and cause immense economic hardship.

In addition, the risk of an electromagnetic pulse or EMP attack remains possible. If a chain is only as strong as its weakest link, then the nation's vulnerability to EMP is perhaps one of the weakest links, making it potentially attractive for foreign adversaries who may seek to cripple the United States without necessarily causing immediate mass casualties. The EMP risk to the nation is well known and has been well documented for years,[3] but is often considered a "low probability" risk despite its potential "high consequence" effects. Again, such dismissals may be dangerously short-sighted.

Third, attacks on the defense industrial base may seriously cripple the U.S. ability to defend the nation and American interests abroad. The defense industrial base is already struggling to produce sufficient equipment to ensure that the U.S. armed forces can successfully meet the growing challenges to U.S. security posed by great powers and rogue state actors.

The defense acquisition process is arguably a mess and has not operated at the "speed of relevance" for many years. The Congress has sought to improve it on multiple occasions, most recently by passing the so-called "SPEED Act" in the House to "restructure, streamline, and modernize the Department of Defense's (DoD) acquisition system."[4] And the Trump Administration is seeking to overhaul the defense acquisition process, giving the Under Secretary of Defense for Acquisition and Sustainment a greater role in managing and overseeing the defense contracting process in ways that streamline bureaucratic

---

[1] Ryan Lucas, "Series of recent DOJ cases show foreign operatives plotting assassinations in U.S.," *KPBS Morning Edition*, February 25, 2024, https://www.kpbs.org/news/2024/02/25/series-of-recent-doj-cases-show-foreign-operatives-plotting-assassinations-in-u-s.

[2] Mark Memmott, "Sniper Attack On Calif. Power Station Raises Terrorism Fears," *NPR*, February 5, 2014, https://www.npr.org/sections/thetwo-way/2014/02/05/272015606/sniper-attack-on-calif-power-station-raises-terrorism-fears.

[3] See, for example, the reports of the congressionally-mandated Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (aka, the "EMP Commission") at https://www.empcommission.org/.

[4] House Armed Services Committee, "The SPEED Act: A Fundamental Reform of the DoD's Broken Acquisition System," 2026, https://armedservices.house.gov/legislation/the-speed-act.htm.

impediments, improve technological innovation, and reduce procurement timelines.[5] Nevertheless, the prospect of adversary attacks on the defense industrial base intended to degrade and delay the procurement of necessary defense articles should not be discounted.

Finally, critical command and control nodes may also be subjected to enemy attack, resulting in the loss of the defense establishment's ability to put force on target as needed. This includes the nuclear command and control infrastructure and enterprise necessary to ensure the effective functioning of deterrence and to execute employment orders should the need arise. It is not beyond the realm of possibility that foreign actors may seek to disrupt or degrade U.S. national decision making and strategic military operations in multiple ways.

Just recently, it was reported that a Chinese intelligence officer owns two golf courses that just happen to be located on both sides of Barksdale Air Force Base in Louisiana, a key strategic bomber installation and part of the Air Force's Global Strike Command.[6] One can only wonder if golf is the only activity taking place there.

Foreign attempts to influence the direction of American policy or damage the American economy are increasingly worrisome. In November, the Department of Justice announced that Chinese nationals – members of the Chinese Communist Party – were arrested for smuggling a biological pathogen into the United States capable of causing severe illness in humans and crop damage costing billions of dollars.[7] In addition, just last week the Royal United Services Institute, or RUSI, released a report noting:

> Sabotage is a key tool of hybrid warfare – and its use is growing. Since 2022, NATO member states have witnessed a marked increase in hybrid operations that have been attributed to Russian military intelligence. There were three times the number of these attacks in 2024 compared with the previous year: the Center for Strategic and International Studies identified 34 incidents of arson or serious sabotage in 2024, compared with 12 in 2023 and just two in 2022….
>
> Russian sabotage covers a range of activity, from intensive operations such as damaging undersea cables to the barrage of low-level attacks against civilian and military targets. Such low-level attacks… are often carried out by ordinary individuals who are recruited via encrypted messaging apps and paid in cryptocurrency.[8]

---

[5] Pat Host, "5 Ways Michael Duffey Is Transforming Defense Acquisition," *ExecutiveGov*, January 8, 2026, https://www.executivegov.com/articles/michael-duffey-pentagon-defense-acquisition-transformation.

[6] Andrew Mark Miller, "National security experts sound alarm over CCP-linked land ownership near US military bases: 'Unthinkable'," *Fox News*, January 8, 2026, https://www.foxnews.com/politics/national-security-experts-sound-alarm-over-ccp-linked-land-ownership-near-us-military-bases-unthinkable.

[7] Department of Justice, United States Attorney's Office, Eastern District of Michigan, *Press Release*, "Chinese National Pleads Guilty and is Sentenced for Smuggling a Dangerous Biological Pathogen into the U.S. While Working at a University of Michigan Laboratory," November 12, 2025, https://www.justice.gov/usao-edmi/pr/chinese-national-pleads-guilty-and-sentenced-smuggling-dangerous-biological-pathogen.

[8] Kinga Redlowska, Marta Popyk and Tom Keatinge, "Responding to Russian Sabotage Financing," Royal United Services Institute (RUSI), January 14, 2026, https://www.rusi.org/explore-our-research/publications/insights-papers/responding-russian-sabotage-

The report cites examples of arson and attacks on civilian infrastructure; parcel bombs and attacks on logistics chains; reconnaissance and vulnerability testing; the vandalizing of symbolic sites and the shaping of local narratives; and the existence of multi-country sabotage networks. And though it focuses on NATO as a whole, it would be shortsighted to assume that these developments do not affect the United States as well.

The point is, regardless of how seriously decision makers wish to consider these threats, or how unlikely we hope they are, there have been numerous incidents that expose the fragility of American infrastructure and the vulnerability of the American economy, political order, and social systems to external actors and interference. These are not trivial concerns.

All of these issues deserve greater attention than they have received. The United States cannot afford another "failure of imagination" if it is to remain the preeminent military power on the planet and maintain the ability to protect and defend the American people and U.S. national security interests.

* * * * * * * * * *

Michaela Dodge
Michaela Dodge is Research Scholar at the National Institute for Public Policy.

I am delighted at the opportunity to join my colleagues David and Chris in discussing this intriguing topic. My argument is that Russia already is at war with the West and it is our own lack of political will to call Russia's activities war. Calling Russia's activities "gray zone" operations or "hybrid warfare" gives us a false sense of security. It makes it more difficult to foster support for the necessary defense budget increases we need to deter increasingly revisionist adversaries. Hope is a danger's comforter, and we have been much too extravagant in hoping after the end of the Cold War.[9]

The term "hybrid warfare," defined as a set of activities below the level of armed conflict, is not useful to describe Russia's activities against the West. In fact, the term masks the severity of Moscow's actual actions and distracts the West from pursuing the kind of retaliatory measures that would lead Russia to pull back from its campaign against targets in North Atlantic Treaty Organization (NATO) states. By evoking the term "hybrid warfare"[10] (or its close euphemisms like "gray zone conflict," "shadow war," or activities "below the level of armed conflict") rather than acknowledging that Russia is, by its own account, at war with the West, gives the impression that the situation is less serious than it actually is.

---

financing?oref=d_brief_nl&utm_source=Sailthru&utm_medium=email&utm_campaign=The%20D%20Brief:%20January%2014%2C%202026&utm_term=newsletter_d1_dbrief.

[9] Paraphrase from Thucydides, *The History of the Peloponnesian War*, quoted in Joel A. Schlosser, "'Hope, Danger's Comforter': Thucydides' History and the Politics of Hope," *The Journal of Politics,* Vol. 75, No. 1 (2013), pp. 169, https://repository.brynmawr.edu/cgi/viewcontent.cgi?article=1022&context=polisci_pubs.

[10] The term originates with the 2006 war in Lebanon. In the context of Russia, it was popularized by Mark Galeotti, who has distanced himself from its contemporary usage. See Lawrence Freedman, "Liberal International Isaiah Berlin Lecture," October 2, 2023, https://liberal-international.org/news-articles/2023-liberal-international-isaiah-berlin-lecture-sir-lawrence-freedman/.

We should see Russia's activities against U.S. allies in Europe as an element of its comprehensive warfare against the West. So far, NATO countries have lacked the political will to impose costs that would dissuade Russia to stop its destructive activities that extend well beyond simply the information sphere. Countering Russia's activities demands a comprehensive response beyond the West's contemporary defensive measures.[11]

Even though Russia's attacks predate its full-scale invasion of Ukraine, just since the start of Russia's full-scale invasion of Ukraine in February 2022, Moscow has conducted over 150 operations on NATO territory.[12] Russia's activities range from assassinations and murder attempts, attacks against NATO's infrastructure, to acts of vandalism through people recruited by Russian handlers via social media.[13] Russia is becoming bolder, with its drones violating Polish airspace in September 2025.[14] Poland in cooperation with NATO allies shot down several of these drones.[15] Russia's drones found their way to Romania. The more immediate goal of the campaign is to weaken Europe's support for Ukraine and to disrupt supply chains through which aid for Ukraine flows.[16] Russia also wants to weaken NATO and undermine the political consensus within the Alliance. Moreover, Russia is the prime suspect in several operations that resulted in cuts to undersea power and communication cables that run across the bottom of the Baltic Sea.[17] So far, we have not seen increases in allies' political willingness to impose punitive measures against Russia, even as Russia is causing billions of dollars' worth of damage. This lack of a punitive response virtually guarantees Russia will continue if not escalate its activities.

While these are not direct attacks on the U.S. homeland, at least not yet, Russia's objective has always been to peel off U.S. allies. Other adversaries will perhaps want to cause chaos in the United States. Our critical infrastructure is vulnerable to acts of sabotage, but also consider that too many so called smart electronic appliances are made in China. It would not be that hard for China to pollute this supply and when useful, give the appliances a command to overheat at the same time. There are only so many firefighting stations across major metropolitan areas. Chinese-made technologies are embedded in many European states'

---

[11] Keir Giles, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power," *Chatham House*, March 2016, https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.

[12] Sophia McGrath, "Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory," The Helsinki Commission, December 2024, p. 3, https://www.csce.gov/wp-content/uploads/2024/12/Spotlight-on-the-Shadow-War-Website.pdf.

[13] Agnieszka Pikulicka-Wilczewska, "'We are here. Join us.' What the trial of two Wagner Group promoters in Poland reveals about Russia's covert campaign in Europe," *Meduza*, April 11, 2025, https://meduza.io/en/feature/2025/04/11/we-are-here-join-us.

[14] Alan Charlish, Lidia Kelly and Barbara Erling, "Poland downs drones in its airspace, becoming first NATO member to fire during war in Ukraine," *Reuters*, September 10, 2025, https://www.reuters.com/business/aerospace-defense/poland-downs-drones-its-airspace-becoming-first-nato-member-fire-during-war-2025-09-10/.

[15] Ibid.

[16] Estonian Foreign Intelligence Service, *International Security and Estonia*, 2025, p. 56, https://raport.valisluureamet.ee/2025/upload/vla_eng-raport_2025_web-002.pdf.

[17] Arno Van Rensbergen, "Hybrid threats: Russia's shadow war escalates across Europe," *The Parliament*, January 21, 2025, https://www.theparliamentmagazine.eu/news/article/hybrid-threats-russias-shadow-war-escalates-across-europe.

infrastructure. One can easily imagine a scenario of these going dark when Russia decides to invade the Baltic states.

Let me end on a quotation: "If the victim does not understand the game, the loss of a pawn here or a knight there does not worry him. If his thoughts are elsewhere, he does not see the traps set for him by his opponent. If his will to win is insufficient, his strength is gradually eroded until, when the tide of combat goes clearly against him, he discovers too late that the price of defeat is intolerably high."[18]

That is why we should call spade a spade, and take our adversaries' word for it—they are at war with us. This is not a Sunday match between your most and least favorite teams. Using clear language will help sustain support for the increased levels of defense spending. It will help our society to become more resilient in the face of threats, thus strengthening deterrence. Punitive retaliatory actions will drain our adversaries' resources and focus and force tradeoffs they otherwise would not have to make.

* * * * * * * * * *

[18] Donald Armstrong, *The Reluctant Warriors* (New York, NY: Thomas Y. Crowell Company, 1966), pp. 180-181.