

# EXPERT EDITION

## Great Power Competition – Taking a Long View

### Insights from

---

- Congressional Research Service
- Defense Department
- International Development Finance Corporation
- Government Accountability Office
- National Defense Industrial Association
- NSF's National Science Board
- National Security Agency
- National Security Commission on AI
- Special Competitive Studies Project



# Secure technology, at scale and speed

Sophisticated global threats require advanced, agile solutions. We are at the forefront of designing and implementing technology that outpace today's adversaries and neutralize tomorrow's threats. We deliver secure technology at scale and speed, from rapid software development to full-spectrum cyber solutions helping ensure our customers are ready for whatever is next. From trusted AI to zero trust, we're harnessing new tools and technologies to advance national security and help our customers protect their assets, information, and citizens at home and around the world.

Find out how we put our high tech on a mission and help our customers protect what's most important.

[leidos.com/capabilities](https://leidos.com/capabilities)



## TABLE OF CONTENTS

Is China more of a threat to the U.S. than Russia? .....	2
The push to broaden AI readiness .....	4
Partnering closely with industry on cyber .....	6
The role of zero trust .....	8
The impact of an evolving defense industrial base .....	10
Investing in developing economies to thwart authoritarianism .....	13
Why security, agility and speed matter in keeping pace with near peers .....	15



## Keeping pace with near peers – more than a military challenge

As I write this, war rages in Ukraine, bringing into stark relief the multitude of challenges that the U.S. government faces – militarily, technologically, economically, to name a few – battling back against aggressor nations that wish to dominate it on the world stage.

Long before Russia began amassing troops and armor along Ukraine’s border, officials across the government were deeply focused on the subject of the great power competition and how best to address near-peer adversaries. China looms large among U.S. leaders’ concerns, in part because its growing economy provides the nation with capital to invest in gaining a foothold against the U.S.

As the Government Accountability Office detailed early in 2021, keeping pace with China illustrates the multifaceted challenges that the Defense Department (and the government generally, to be fair) faces in competing globally.

“The good news is that DoD knows this and is taking action, although our work has found that DoD will need to continue its course and strengthen its capabilities to be best positioned to face this threat,” notes Cathy Berrick, managing director of GAO’s Defense Capabilities and Management Team.

Defense leaders and others across government realize that the country must take a long view and that it also must look beyond just military might, which while a critical element is not the only factor in the U.S. maintaining its standing globally.

In the pages ahead, we hope to provide a look at the breadth of the challenges as well as offer some insights about how federal agencies and organizations are tackling or plan to tackle the great power competition.

**Vanessa Roberts**  
**Editor, Custom Content**  
**Federal News Network**



# DoD faces challenges in maintaining global footing with China and, to a lesser degree, Russia



BY VANESSA ROBERTS

The idea of the United States countering China and Russia to ensure dominance globally is not new in concept, but it's certainly gained traction the past few years. It has been referred to as the great power competition or the strategic competition – and the countries as the U.S.' near peers.

Defense Department officials contend that countering China's military capabilities is DoD's top priority, the Congressional Research Service noted in a [report](#) updated in late March. Russia's military, particularly its nuclear arsenal and biological weapons capabilities, also rank among DoD's concerns. (Russia's invasion into Ukraine has provided much new intelligence about its military.) But China's "economic growth since the 1990s enabled the country to make significant investments in its military, economic and development power," pointed out the Center for Strategic and International Studies in its own March 2021 [report](#).

Russia, because of its limited economic and development power, "poses far less of a multifaceted challenge to the United States," the CSIS report said.

But staying ahead of either of these authoritarian countries is not exclusively about managing military might and troops. There's also a need to address R&D and technology developments to respond to cyberthreats and to ensure advanced capabilities like artificial intelligence and quantum computing.

"AI is a critical technology that likely is going to have significant implications for many more fighting functions – from logistics to intelligence activities and really everything in between," noted Cathy Berrick, managing director of the Defense Capabilities and

Management Team at the Government Accountability Office, while discussing the [national security snapshot](#) on China that her team released in February.

"China recognizes this and views AI as critical to its future military and industrial power and is investing very heavily in AI," she added, as must DoD.

## Defense faces multiple strategic competition challenges

In its national security snapshot, "Challenges Facing DoD in Strategic Competition with China," GAO underscored the multipronged demands on DoD. Although the snapshot focus was on China, GAO listed five top-level challenges that could broadly apply to either of Defense's near-peer adversaries:

- Anti-access and area-denial: "long-range precision strike capabilities (ballistic and cruise missiles) able to reach U.S. logistics and power projection assets"
- Surface and undersea operations: "offensive and defensive capabilities aimed at gaining maritime superiority"
- Cyber: "capabilities as a tool to deter or degrade an adversary's ability to conduct military operations"
- Space: "the ability to use space-based systems – and to deny them to adversaries"
- Artificial intelligence: "critical to future military and industrial power."

In essence, GAO concluded that all five are areas that DoD acknowledges it must act to maintain pace with China and that none can really take a back seat to the others.



## Troop distribution and shifting military priorities

For more than a decade, there have been discussions of redistributing the U.S. military presence abroad, both to reduce the need to sustain those operations and instead deploy to a region as a crisis demands and also to address China's growing military strength. The department has considered moving more troops to the Indo-Pacific region as a deterrent.

But the Russian invasion of Ukraine raises new concerns. As the Congressional Research Service pointed out: "Russia's recent actions in Europe and developments in the Middle East pose their own security challenges, and some observers express concern about a scenario in which the United States could face major military contingencies in multiple parts of Eurasia in rapid succession or simultaneously – a consideration that can complicate plans for shifting U.S. military capabilities from Europe or the Middle East to the Indo-Pacific."

## Budgets lag planning

Funding programs aligned to the great power competition have also been a challenge, noted CSIS' George Sanders in an [interview](#) with Federal News Network's Jared Serbu.

There's a "little bit of a gap" between funding and areas identified as high priorities in the department's strategic competition plans, said Sanders, who is deputy director of the center's Defense Industrial Initiatives Group. He attributed that largely to inertia in the processes at the department, although he does see some shifts happening through the use of other transaction authorities (ATOs) to make purchases.

Even so, established programs still have "a great deal of pull and the attempt to move toward what's newest and [has] priority is slow in coming," he said based on a CSIS review of unclassified budget documents from fiscal 2017 through 2020.


That said, the CSIS review did note some positive signs, Sanders said. "We have seen a real jump in ships and submarines that I think for some of the

**"Russia's recent actions in Europe and developments in the Middle East pose their own security challenges, and some observers express concern about a scenario in which the United States could face major military contingencies in multiple parts of Eurasia in rapid succession."**

– Congressional Research Service, "Renewed Great Power Competition: Implications for Defense – Issues for Congress"

larger fleet goals, you can see that alignment; aircraft continue to be up. But on electronics, communications and sensors, that's still pretty flat," he said. "And the other thing that happened [in] 2020 was a massive jump in other transaction authority spend. But a lot of that was driven by vaccine purchase rather than defense strategy purposes."

The Congressional Research Service also pointed to funding to support space and cyber initiatives, specifically the creation of Space Force and of the U.S. Cyber Command as a distinct combatant command within DoD.

"There's unfortunately no silver bullet solution," GAO's Berrick said. "The good news is that DoD knows this and is taking action, although our work has found that DoD will need to continue its course and strengthen its capabilities to be best positioned to face this threat. And continue congressional oversight will be important as they do. I really don't think it's an understatement to say that strategic competition with China is unlike any other challenge DoD has faced." 

# Federal R&D investments serve as foundation for US to become AI-ready

BY JORY HECKMAN

The National Security Commission on Artificial Intelligence, in its [final report to Congress and the Biden administration](#) last year, warned that artificial intelligence would soon become weapon “of first resort in future conflicts.”

That warning, as well as the commission’s recommendation for the federal government to double down on its R&D spending, remain urgent for the United States to remain AI-ready in the coming years, even though the commission no longer remains.

The commission disbanded in October 2021, but many of its leading experts have shifted to a private-sector entity, the Special Competitive Studies Project.

## Taking a page from world history

SCSP’s name stems from the Rockefeller Special Studies Project, launched in 1956 by Nelson Rockefeller and Henry Kissinger following the Soviet Union’s launch of the satellite Sputnik.

SCSP Chief Executive Officer Ylli Bajraktari, the commission’s former executive director, said Rockefeller and Kissinger saw their project as a way for the U.S. to further define its national objectives when it came to defense, security and foreign policy.

“This is not the first time that we’re seeing technology playing a critical role in great power competition,” Bajraktari said.

That mission, he added, remains urgent in the present day. Unlike the Cold War era, however, when the federal government played a leading role in R&D, the private sector is now the driving force in such spending.

Private sector research investments have obvious impacts on society and the public but also hold major implications for national security, Bajraktari said.

**“This is not the first time that we’re seeing technology playing a critical role in the great power competition.”**

– Ylli Bajraktari, CEO, Special Competitive Studies Project

“That why this is such a critical time, because of the diffusion of power, the diffusion of technologies. ... Anybody can purchase these kind of capabilities off the shelf or online. This is new momentum in how conflicts are waged,” he said.

To prepare for the next era of great power competition, Bajraktari said the federal government will need to increase its level of spending on basic R&D.

## Strategic dominance requires government investment

In its final report, the AI commission urged Congress to double federal R&D spending on AI each year with the goal of reaching \$32 billion in fiscal 2026.

“If we don’t outmaneuver and not out-innovate China, we will not be in the lead position when it comes to these emerging technologies,” he said. “The lead position in emerging technologies ensures that our economy keeps progressing, that our society is using all the benefits from these technologies, and ultimately, our military has the latest and greatest capabilities, if they need to utilize it for the warfighting purposes.”

## NSB: Our competitors are closing the gap

Meanwhile, the National Science Foundation's National Science Board, finds the U.S. remains strong in terms of global R&D competition, but global competitors are catching up.

Victor McCrary, NSB's vice chairman and the vice president for research and graduate programs at the University of the District of Columbia, said the U.S. "still outpaces everybody in terms of overall, global R&D."

However, McCrary said South Asian and Southeast Asian countries, particularly China, have seen a significant uptick in R&D spending.

"While the U.S. leads, that margin between us and our nearest competitors is starting to close, and I think that's a concern from the White House to the Congress, to many of our businesses, universities, as well as well as the military," McCrary said.

Basic R&D served as the foundation for breakthroughs in artificial intelligence, quantum information systems, 5G, biotechnology and advanced manufacturing, he said.

The National Science Board, under the National Science Foundation Act, is required to send Congress and the president a report on the state of science and engineering every even-numbered year.

This [year's report shows](#) that in addition to being a top global spender on R&D, the U.S. maintains a competitive advantage by still drawing the best talent to its universities and companies.

McCrary said that talent pool gives the U.S. an international advantage.

"We still have the best companies in the world when it comes to AI applications and integration of these things," he said.


But, Bajraktari added, maintaining a high level of R&D spending is also a vital part of developing the workforce necessary to remain competitive.

"If these are our comparative advantages, then I think basic R&D can help toward incentivizing students and Ph.D. candidates at universities to come up with next-generation AI capabilities," Bajraktari said.

## Building a next-generation workforce

However, federal agencies need to do a better job of ensuring private sector tech experts have opportunities to lend their expertise to the government through short-term tours of duty, he suggested.

Meanwhile, he said the Defense Department and the intelligence community need to develop clearer career pathways for AI and emerging tech experts to stay in federal service.

"The career path inside a federal agency is not clear cut if you have a technology background. Until yesterday, this was considered an IT issue, but this is no longer an IT issue," Bajraktari said. "We need the military to understand that if somebody comes with a coding background, you have to incentivize them and create a career pathway for them to stay there and get promoted and get incentivized – not move them around every two to three years, like we do right now. Because otherwise you will lose the benefit of these individuals coming with these skills." 

**"While the U.S. leads, that margin between us and our nearest competitors is starting to close, and I think that's a concern from the White House to the Congress, to many of our businesses, universities, as well as well as the military."**

– Victor McCrary, Vice Chairman,  
National Science Board



# Through unclassified collaboration center, NSA partners with industry to better respond to foreign cyberthreats

BY VANESSA ROBERTS

The National Security Agency has taken a decidedly transparent tack when it comes to keeping pace with U.S. competitors in the realm of cybersecurity threats. Over the past year, NSA stood up the Cybersecurity Collaboration Center to work directly with industry partners on sharing threat information.



“We see a significant amount of cyberthreats originating every day from our foreign adversaries,” Adamski said.

She expects that the center’s budding relationships with the private sector can help the government and industry improve the nation’s cybersecurity standing.

“The Cybersecurity Collaboration Center is actually this very unique unclassified facility, outside of the fence line right off of 295, that our partners are able to come visit us, share what they’re seeing in real time, and we’re able to share our insights as well,” the center’s director, Morgan Adamski, told Federal News Network’s Tom Temin during an interview on [The Federal Drive](#).

Of course, given that NSA opened the center amid the COVID-19 pandemic and has partnerships with more than 100 industry members across the country, a lot of activities have been virtual, Adamski said.

“We do things like chats, and just say, ‘Hey, here’s what we’re seeing,’ ” she said. “It’s not typical for NSA to be in an open environment and collaborating at the unclassified level. This is really the dramatic change for us.”

## Speeding U.S. response to cyberthreats

NSA created the center in response to the Biden administration [executive order on improving cybersecurity](#) to focus on threats from external bad actors that could cripple the country.

“The unique thing about NSA in the Cybersecurity Directorate is we’ve really brought together the power of understanding the foreign nation state cyberthreats with understanding the defensive space,” she said. “And when we bring together both the threat information with understanding vulnerabilities, you build this magical system of being able to put mitigation in place quicker.”

## Collaborating closely with CISA too


NSA has no intention of overstepping into the authority of the Cybersecurity and Infrastructure Security Agency at the Homeland Security Department, Adamski was quick to add. That said, the agency shares what it learns with CISA too.

“Obviously, they have the mandate and mission to reduce the risk to the national and critical infrastructure,” she said. “We have a fundamental understanding of the foreign cyberthreats. And when you bring those two narratives together, what you’ve really created is scope, span and being able to talk to our industry partners.”

The result? The center and CISA communicate almost daily, Adamski said.

The potential for these relationships is already clear and has the potential to help with development of the [Enduring Security Framework](#), a cross-sector initiative that aims to address risks that threaten critical infrastructure and national security systems.

“Our industry partners see a lot of malicious activity on any given day. They see it; they have a lot of noise on their networks. They may not understand it; they may not know who’s responsible for it,” Adamski said. “They have part of the picture – just like NSA. We have part of the picture as well.”

The collaboration center brings the varied pieces together to “get a better understanding of what the comprehensive picture looks like,” she said. “It’s really about drilling down into those threats and being able to have a conversation.” 

**“It’s not typical for NSA to be in an open environment and collaborating at the unclassified level. This is really the dramatic change for us.”**

– Morgan Adamski, Director of the Cybersecurity Collaboration Center, National Security Agency

**+100**

**Industry partners that work with NSA to exchange threat insights through the agency’s Cybersecurity Collaboration Center**

SOURCE: [“What the NSA has learned from a year of external cybersecurity collaboration,”](#) Federal News Network, February 2022

# 3 cybersecurity tactics that agencies can take to thwart new 'whole-of-nation' attack vector

PROVIDED BY LEIDOS



**Doug Jones, Chief Technology Officer for Defense, Leidos**

A number of U.S. officials and federal agencies have been sounding the alarm on cybersecurity since the lead-up to Russia's invasion of Ukraine. But Russia has been testing cyber capabilities in Ukraine for years, such as its attacks on Ukraine's power plants. The current conflict has simply driven home the fact that cyber is truly

a warfighting domain, and agencies need to be prepared to engage on this front.

"There's a lot of active war going on in the cyber domain that is more aggressive than people see in the classic kinetic sense," said Doug Jones, chief technology officer for Defense at Leidos. "Some folks also view cyber as a de-escalation technique. If Russia wanted to try to prevent us from getting involved, they may use cyberattacks to say, 'Do you really want to get involved in this? Because we could actually take down some of your critical infrastructure and take the fight to your home,' as opposed to it being in Europe."

There are three key elements agencies need to adopt to survive on this new battlefield: zero trust, resilience and adversarial thinking.

## Tactic 1: Zero Trust

Zero trust is not something agencies can just buy; it's a philosophy, an architectural paradigm, Jones said. It requires implementing multiple layers of defenses, along with adopting a transactional approach to trust, rather than a permanent one.

That involves factoring risk into the decisions about who (or what in the case of devices and other nonhuman components) to trust, when to trust them and with what data.

So how can agencies modernize into that architecture?

Incrementally, Jones says.

Every agency is going to be different. It's going to have different goals, different needs and a different starting point. Each of these will influence where an agency needs to begin prioritizing zero trust. That's why Leidos came up with the Zero Trust Readiness Level, to help agencies evaluate where they stand and what their next steps should be.

"Where are you from an identity and access management, multi-factor authentication or networking perspective? Are you ready to get into microsegmentation? Where are you on your application layer?" asked Jones. "As we start understanding where you are, we can put up where you are on the Zero Trust Readiness Level, and then figure out what is a custom plan based on the outcomes you want to achieve to get to the next level."

The idea is to help organizations get closer to their specific cybersecurity needs relative to achieving zero trust, he said. That way "rather than saying, 'I need this product because it'll help me get to zero trust,' now I can say, 'I need a suite of these products to solve these five problems because these are the best products to solve those problems, given my infrastructure and my architecture, to get me to the next level of maturity from a zero trust perspective.'"



## Tactic 2: Resiliency

By adopting a zero trust posture through a more focused approach, agencies will be able to develop resiliency, Jones said. Using a maturity model will allow them to be more agile and flexible in responding to unanticipated situations, he said. In the past, much of cybersecurity has revolved around compliance. But compliance is just a snapshot in time; it's easy to quickly fall into obsolescence, Jones warned. Zero trust, on the other hand, is about understanding the risk associated with every area of a business and then mitigating that risk.

For example, a classic cybersecurity approach would be to have a disaster recovery system. But that's just checking a box, he said. A more modern solution calls for implementing multiple active systems running across various cloud service providers in tandem, so they can seamlessly pick up workloads and reduce risk. Similarly, agencies should be considering how to prevent other types of risk, from supply chain to architecture and monitoring, Jones advised. Agencies need to consider the tools at their disposal to deal with these kinds of risk.

## Tactic 3: Adversarial thinking

Once agencies have established a zero trust architecture and implemented the appropriate risk response tools, they need to start thinking like their adversaries to better know how to

deploy them. And those adversaries could be anyone, from near-peer competitors to organized cybercrime organizations and hackers. "The thing we always want to think about is what would someone want with my organization's network or data? Or how would they want to disrupt my mission?" Jones said. "The question is: What are they going to attack? Do they want to take you down? Do they want to prevent you from doing your mission or degrade your mission? Do they want to prevent the integrity of your data so you don't trust it?"

The key is to understand the value of the data or access to the agency's systems to potential adversaries, he explained. There may be more than one answer. For example, attacks that compromise personally identifiable information, like the Office of Personnel Management breach or attacks on insurance companies, allow adversaries to build dossiers of trusted individuals in various positions of authority and access. How could that data then be leveraged?

"When you look at classic cyber, they talk about something called the CIA triad. That's not the intelligence service; that's confidentiality, integrity and availability," Jones said. "We're seeing this whole-of-nation attack vector. It goes back to what would I want to do as an adversary to you to either get your data, prevent you from accomplishing your mission or create distrust in your mission?"

**"There's a lot of active war going on in the cyber domain that is more aggressive than people see in the classic kinetic sense."**

— Doug Jones, Chief Technology Officer for Defense, Leidos

# Defense contractor revenue is strong, so why is the state of the sector weakening?

BY JASON MILLER

The Defense Department's mandated report from President Joe Biden's July executive order on [promoting competition](#) would lead you to think the shrinking supply chain is putting the nation at risk.

"Since the 1990s, the defense sector has consolidated substantially, transitioning from 51 to five aerospace and defense prime contractors," the [February report](#) stated. "As a result, DoD is increasingly reliant on a small number of contractors for critical defense capabilities. Consolidations that reduce required capability and capacity and the depth of competition would have serious consequences for national security."

A week before that report dropped, the National Defense Industrial Association rang alarm bells that played a similar tune.

NDIA's "Vital Signs 2022" report found the health of the defense industrial base (DIB) at its lowest point since the [launch of the review](#), with five of eight categories falling below a passing grade of 70 out of 100.

"Vital Signs 2022 also reflects the story of recent political and regulatory action against adversaries and their influence over the DIB, and the way in which that has shaped and will continue to shape the future of the warfighter," NDIA and Govini [found in the report](#). "This past year has witnessed significant

**"We won't have the next set of emerging technologies if we're not investing in the basic research."**

— Mark Lewis, Executive Director, NDIA's Emerging Technologies Institute

deterioration in the signs including 'supply chain' as well as 'production capacity and surge readiness,' which almost certainly is a result of the impact of the pandemic. Conversely, the only sign that significantly improved was 'demand,' reflecting recent growth in the Defense budget."

But these reports really only tell one side of the story.

## DIB contractors see rise in revenue

Conversely, the data on overall spending, the rate of competition and the total revenue all point to an industrial base that is healthy, wealthy and, hopefully, a little wiser.

Bloomberg Government found in its fiscal 2020 report — the most recent data available — that most of the top 10 contractors across government, not just within DoD, saw their revenue increase over the previous year.

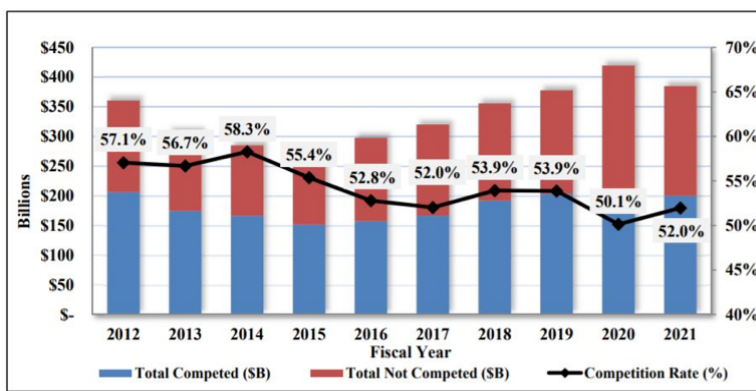
Lockheed Martin, for example, repeated as the top contractor in 2020, bringing in \$75.8 billion in federal contracts, up from \$43.4 billion in 2019. In 2021, NDIA reported Lockheed earned \$74.9 billion, while the next four DIB vendors, Raytheon, General Dynamics, Boeing and Northrop Grumman all saw decreases between 2020 and 2021.

It's not just about straight revenue either. DoD reports that the overall competition rate among contractors reached 52% in 2021, more than 1% higher than 2020, but lower or equal to the rate each year since 2012.

The increased competition rate along with the revenue increases comes despite growing concerns about mergers and acquisitions negatively impacting the price for specific products like major weapons systems as well as the availability of products and services.

“Although studies of this trend have not found a strong correlation between consolidation and increased program pricing, additional risks beyond pricing come with consolidation,” DoD stated. “Growing concentration can reduce the availability of key supplies and equipment, diminish vendors’ incentives for innovation and performance in government contracts, and lead to supply chain vulnerabilities.”

The DoD and NDIA reports are part of a growing drum beat across the defense sector warning lawmakers about the increasing near-peer competition coming from China, Russia and other countries – and whether the [defense industrial base](#) can keep ahead of them.



Note: Dollars shown in billions

Figure 1: Ten-year trend for DoD competitive and non-competitive dollars

SOURCE: “[State of Competition Within the Defense Industrial Base](#),” Defense Department, February 2022

As Congress looks to begin to work on fiscal 2023 spending bills, the reports highlight both real and perceived threats for lawmakers to consider as they parse out the more than \$700 billion DoD budget.

“Many of these challenges were there before COVID. The pandemic served to highlight and accelerate these challenges. But it is definitely a wake-up call for the decision and policymakers in our country,” said retired Air Force Gen. Herbert “Hawk” Carlisle, president of NDIA, during a press briefing in early February. “The aggressive Russian military buildup on the Ukrainian border and the pacing threat, the rapid military modernization efforts of the People’s Republic of China remind us that our industries work, of providing superior products and services to armed services so that they can compete and win in all domains of warfare, can never be taken for granted. We owe it to the women and men that serve and defend this nation to give them the equipment, the capability and the training to do the mission we asked them to do. Right now, in the environment we’re operating in, it’s a challenge, and we’ve got a lot of work to do.”

## Chinese investment in AI

The “Vital Signs 2022” report should prompt DoD, Congress and the White House to better understand how challenging the current federal procurement environment has become over the last decade, said Tara Murphy Dougherty, CEO of Govini.

“DoD has to attract the companies that are working on bleeding-edge technology in the commercial sector of the United States economy,” Murphy Dougherty said. “If we cannot accomplish that, the techno-military challenge and competition that we’re facing with China will continue to undoubtedly get more difficult. If you consider comparative investments between the United States and the Chinese Communist Party in these emerging technologies, and the commitment that China has to leveraging those technologies for warfare, it’s clear what DoD needs to do. That begins by improving the environment in which these companies operate in order to serve DoD and the national security efforts of our country.”



## From 51 to 5

# Consolidation of prime weapons contractors in the U.S. over the past 30 years

SOURCE: “[State of Competition Within the Defense Industrial Base](#),” Defense Department, February 2022

It’s the concern about the gains China and Russia are making that is helping to drive this mixed message about the DIB.

Both reports found the number of new entrants coming into the defense sector has steadily dropped. DoD says the reduction is felt most among weapons suppliers, which fell to five from 51 in the 1990s. The lack of new entrants into the DIB is surprising and concerning, especially during the pandemic, said Wes Hallman, senior vice president for strategy and policy for NDIA.

“Two different studies, one from 2008 to 2018 and one that was 2011 through 2018, noted thousands of companies have left the defense industrial base,” he said. From 2019 to 2021, new entrants in the DIB fell from 12,000 to 6,300.


“As policymakers look at this, we need to look at what are the incentives and disincentives to come into this marketplace and really adjust the marketplace so it’s easier to enter it, easier to thrive in it and then produce some resilience.”

## More vendors in R&D defense sector

Carlisle added that the drop in new entrants comes despite the defense sector being somewhat protected against the economic challenges brought on by the pandemic.

The one area that has bucked this shrinking trend is R&D, where the use of other transaction authority has increased the number of vendors by 9% over the last decade, DoD reported.

Mark Lewis, executive director of NDIA’s Emerging Technologies Institute, said DoD must reverse the spending decline on basic research as a way to address many of these growing DIB problems. “We won’t have the next set of emerging technologies if we’re not investing in the basic research,” Lewis said. “I think we can certainly highlight some successes of the Defense Innovation Unit, which has been incredibly successful at kind of opening the door for new companies to come into DoD.”

But the department needs to push forward and get behind a consistent message, he added. “There’s a sense of alacrity, but again, we’re getting some mixed messages along those lines. So it remains to be seen. We’ll certainly see when the 2022 National Defense Strategy is released if it continues to emphasize the importance of these emerging technologies, and especially with a focus on peer competitors such as Russia and China.” 

**“DoD has to attract the companies that are working on bleeding-edge technology in the commercial sector of the United States economy. If we cannot accomplish that, the techno-military challenge and competition that we’re facing with China will continue to undoubtedly get more difficult.”**

– Tara Murphy Dougherty, CEO, of Govini

# U.S. agency takes aim at authoritarianism through economic support in developing countries

BY VANESSA ROBERTS

Not every effort by the U.S. government in the great power competition involves military capabilities. In fact, a significant piece of the puzzle focuses on bolstering the economies of developing countries through direct financial aid to struggling businesses and local government programs.

A prime example is the International Development Finance Corporation (DFC). “We are driving investments in the private sector throughout the developing world to raise living standards, to advance American foreign policy interests and to aid those countries in development,” said David Marchick, who spoke with Federal News Networks’ Tom Temin on [The Federal Drive](#) shortly before stepping down as DFC’s chief operating officer.

In fact, a chief reason for the formation of the new organization in 2019, spelled out in the Better Utilization of Investments Leading to Development (BUILD) Act, is to respond to China’s increased economic influence in developing countries through its Belt and Road Initiative.

The law does not mention China, or any near-peer countries by name, but does point out that DFC will ensure “a robust alternative to state-directed investments by authoritarian governments and strategic competitors using best practices with respect to transparency and environmental and social safeguards, and which take into account the debt sustainability of partner countries.”

The agency was built from what was formerly the Overseas Private Investment Corporation. The



BUILD Act doubled the agency’s investment capacity from \$30 billion to \$60 billion, added additional tools and also brought over certain aspects of the U.S. Agency for International Development, Marchick explained. “Now, we’re essentially America’s development bank.”

*(Read more about the BUILD Act and DFC’s founding in this [Congressional Research Service report](#).)*

## A long-game mission that matters

Its DFC’s broad effort to advance foreign policy and national security interests that has helped make the nascent agency successful, Marchick said. Battling back against dictatorships and maintaining the United States’ competitive advantage on the world stage “is one of the essential goals of the BUILD Act and why Congress, on a broad bipartisan basis, supports DFC,” Marchick said.

And DFC takes this part of its mission very seriously, as Chief Development Officer Andrew Herscowitz explained during a March hearing of the Senate Foreign Relations Subcommittee on Western Hemisphere, Transnational Crime, Civilian Security, Democracy, Human Rights and Global Women’s Issues.

“DFC’s model is to mobilize private capital in a way that upholds the highest social and environmental standards, reinforces good governance, avoids unsustainable debt levels, promotes inclusion, and contributes to sustainable and broad-based economic growth in the areas we work,” noted Herscowitz

in his testimony. “That is a value proposition our competitors are unable to offer, and we believe our values and practices set DFC apart as a much better partner for developing countries.”

In particular, he noted that such investments are a direct counter to recent engagements by China in the Caribbean and Latin America, where DFC has invested more than \$10 billion in agriculture, financial services and healthcare resiliency programs.

“Unlike the Peoples Republic of China, DFC’s efforts seek to empower our partner countries, helping them take advantage of and control their own resources. DFC’s model is one of partnership and empowerment – not one of taking and exploiting,” Herscowitz said.

China mainly finances organizations that it controls or creates unsustainable debt for governments in the regions, he said. “The DFC model allows us to provide financing directly to the people and businesses in Latin America and the Caribbean.” The agency intends to continue to expand these efforts, Herscowitz added.

## How DFC programs work in practice

Herscowitz and Marchick both offered some specific examples of projects underway in Latin America.


One example that typifies DFC’s infrastructure objectives is taking place in Brazil, Herscowitz told lawmakers. The agency has agreed to pump up to \$267 million into a project to modernize the public lighting system and install a smart city infrastructure in Rio de Janeiro.

**“The DFC model allows us to provide financing directly to the people and businesses.”**

– Andrew Herscowitz, Chief Development Officer, DFC

“The project will lead to energy savings of 60% per year compared to the current system through the retrofit or addition of 450,000 public lighting units with LED technology,” he said. “The smart city infrastructure will include 4,000 remote sewage monitors to aid in adaptation to and resilience against flooding risks, 6,000 smart traffic lights and 5,000 public Wi-Fi access points. Nearly three-quarters of capital expenditures of the project will flow to neighborhoods below the city’s median income.”

What’s more, the Smart Rio team that won the work, and which DFC is supporting, beat out two other bidders, one a Chinese consortium backed by Huawei Technologies, Herscowitz said.

Marchick shared another effort supporting the Venezuelan migrant community in Colombia, where many Venezuelans relocated after leaving their country to escape political and economic turmoil. DFC is providing financial support both to the migrants but also to the communities that are hosting them, he said. “We want to work with our partners throughout the world to support economic freedom, to support opportunities and to strengthen democracy.” 

**\$6.7 billion**

**What DFC invested in fiscal 2021, which is 60% more than the average over the past five years**

SOURCE: [“Meet the new chief operating officer of an agency that’s only two years old.”](#)  
Federal News Network, November 2021



# Great power competition requires security, agility, speed

PROVIDED BY LEIDOS



**Jim Carlini, Chief  
Technology Officer,  
Leidos**

American military and foreign policy doctrine has changed in the last several years as the world situation has changed.

Now, the idea of a great power competition has emerged as China and Russia demonstrate ever-rising willingness and ability to challenge

the supremacy of the United States.

Doctrinal and policy changes mean — down at the function levels of government — that activities and supporting technologies must adapt too. According to Leidos Chief Technology Officer Jim Carlini, broad-based integrators and technology vendors are working to ensure their products and services match this emerging need.

The definition of great power competition itself is still developing, Carlini said during an [interview](#) with Federal News Network's Tom Temin.

"The current administration, for instance, likes 'strategic competition' versus 'great power competition,'" he said. "But by whatever name you prefer, it's a label really for a new era of geopolitical jockeying for influence and control of global affairs."

## A governmentwide concern

Moreover, it's not just a Defense Department issue.

"It cuts across things like diplomacy, economic, military, information, intelligence, law enforcement — all of those levers of power get touched," Carlini said. "It touches the entire government," including Defense, the intelligence community, and the Commerce, Homeland Security and Treasury departments.

Large technology integrators have what Carlini called a privileged position in helping the government navigate its way to readiness in this new era of conflict.

One way is by bringing deep understanding of commercial technologies and bridging them to specific governmental needs.

**"Every domain is contested in a great power competition, whether it be defense applications or civil and health applications. We need to protect the critical infrastructure for the nation. So security is a major theme that we as a system integrator bring to our customers."**

— Leidos CTO Jim Carlini

For example, the government might need privacy assurances, auditability and rapid deployment “to serve some of their mission purposes from warfighting to simply gaining efficiencies that are very important for reducing expenditures, and allocating some of that money toward mission and for great power competition,” Carlini said.

Another way is by enabling greater resilience and security to agencies and the data crucial to their missions. “Security is a major theme that we as a system integrator bring to our customers,” he added.

Competing nations have started to deploy artificial intelligence – in some cases against one another. Carlini said an important U.S. requirement is that such technologies be used, for whatever purpose, in a way that respects U.S. values and laws.

### The zero trust connection

AI and cybersecurity intersect in the great power competition, as the need for data and intellectual property protection becomes ever more crucial. Carlini said Leidos’ zero trust proving ground – a methodology for

discovering how zero trust architectures, technologies and components perform – can help. Furthermore, the applications of zero trust apply beyond networks to many forms of complex systems, including a growing number of unmanned and autonomous systems in development by the U.S. military.

“And we’re also bringing AI into zero trust, to have better algorithms for determining how to manage a zero trust–resilient architecture, Carlini said. “And we’re using AI with cyber to more quickly come up with better defensive applications and to counter the advanced threats, those that come from state actors that are very, very good and tend to hide in networks.”

Another capability Leidos is working on for the Defense Department is hypersonic weaponry. The topic has spawned many headlines as both China and Russia appear to show off hypersonic developments, including a claim in March by Russia that it deployed hypersonic missiles during attacks within Ukraine.

Leidos is building what Carlini called a hypersonic glide body at its Dynetics facility in Huntsville, Alabama. “We need to move with speed in order to make sure we’re competing in the hypersonics realm,” he said.

In fact, the need for speed permeates nearly everything the government does in the great power competition, Carlini said. He cited Air Force Chief of Staff Gen. Charles Q. Brown Jr.’s paper, “[Accelerate Change or Lose](#),” as an example of the call for moving more quickly and with more agility.

“So the alarm bells are going off. And that is all about being able to move very rapidly from this point forward,” Carlini said. “We need to innovate with speed. And we need to do that across the board, across all the domains.”

**“We’re very much in the hypersonic domain at Leidos. It’s a very important development and a very important area. The combination of speed, maneuverability and altitude with hypersonic weapons really makes them potent.”**

– Leidos CTO Jim Carlini