DEFINING OUR FUTURE

THE CAMPAIGN IN SUPPORT OF
THE UNITED STATES AIR FORCE ACADEMY

NO-FAIL MISSION

GLOBAL ADVERSARIES ACTIVELY EXPLOIT NATIONAL VULNERABILITIES

A WHITE PAPER ON THE FUTURE OF CONFLICT FOR THE UNITED STATES

NO-FAIL MISSION

BY JEFF HOLMQUIST

In the summer of 2020, United States Air Force Chief of Staff Gen. CQ Brown Jr. offered a stark warning:

"The nation's adversaries are rapidly expanding their capabilities in conventional and non-conventional warfighting domains, and the U.S. is in danger of falling behind."

Throughout much of 2021, media reports indicated that near-peer competitors, such as China and Russia, were flexing their muscles and unafraid of flaunting some of their advances.

In early 2022, an emboldened Russia — buoyed by advances in cyber, space, hypersonics and more — invaded Ukraine and has provided the globe a glimpse into what the future fight entails.

Since issuing his warning, Gen. Brown's newly coined phrase — "Accelerate Change or Lose" — has become a rallying cry among those intent on returning our nation to dominance on the global stage. Gen. Brown was communicating with Air Force personnel at the time, but the idea has come to resonate across the Department of Defense.

"If we do not change — if we fail to adapt — we risk losing the certainty with which we have defended our national interests for decades," Brown says.

For much of the last century, our nation's military could boast dominance in the air, on the sea and over land. But recent developments in space, cyberspace, electronic warfare, misinformation/disinformation campaigns, unmanned aircraft and artificial intelligence have left the U.S. vulnerable to any number of adversaries around the globe.

"We are being more effectively challenged than at any other time in our history," Secretary of the Air Force Frank Kendall said at the Air Force Association's 2021 Air, Space & Cyber Conference.

SETTING THE STAGE

Lt. Gen. (Ret.) Bradford Shwedo, director of the Institute for Future Conflict and USAFA Class of 1987 graduate, traces the challenge to U.S. superiority back to Sept. 11, 2001.

In the 20 years since the terror attacks, our nation's adversaries have invested heavily in a two-pronged approach to competing against the U.S. — asymmetrical (aka unconventional) attack axes such as cyber, space and artificial intelligence plus expanded conventional warfare capabilities.

Unfortunately, our nation's defense strategy during that same period shifted.

"We were going down the road of Great Power Competition," he recalls. "Then, all of a sudden, we started focusing on Al-Qaeda, the Taliban and, later, ISIS. In the battle for finite resources, as we started to reduce our counterterrorism efforts, we found our previous investments and focus left us ill-equipped for Great Power Competition."

Because global terror organizations did not have effective abilities in electronic warfare and space, the military budget reflected a higher priority on lower-technology adversaries.

As the Global War on Terrorism dragged on, the focus on extremists allowed our Great Power adversaries to make gains and, as a consequence, both symmetrical and asymmetrical attack axes grew more pronounced with every budget cycle, according to Gen. Shwedo.

With the end of the Afghanistan War in 2021, the U.S. strategy has again returned to the growing threats from near-peer competitors.

Gen. Shwedo is energized by Gen. Brown's challenge to "Accelerate Change or Lose." A refocused National Defense Strategy and a corresponding shift in budget priorities, he says, are required to regain and maintain the nation's military dominance.

"The chief of staff and the chairman of the Joint Chiefs of Staff ... are seeing what others are seeing, and they're telling us we have to get ready," he says.

RUSSIA

Russia conducted a missile test on Nov. 15, 2021, blowing up one of its own satellites orbiting the Earth. The resulting debris field endangered astronauts and cosmonauts on the International Space Station.

"Since about 2007, potential adversaries — specifically the Chinese and Russians — have noticed how effective we use space in military operations," reports Gen. David Thompson, vice chief of Space Operations for U.S. Space Force and USAFA Class of 1985 graduate. "They have begun to develop and build weapons systems that take those capabilities away from us."

After the test of its anti-satellite technology, Russia warned via state television that it now has the capability to blow up the 32 satellites that make Global Positioning System (GPS) possible. The United States Space Force is scrambling to better defend the system.

CHINESE J-20 STEALTH FIGHTER

In the decades since development of GPS, the military and society in general have come to rely heavily on the technology, including with supply chains. If the satellite-based system was ever knocked out by an adversary, it could pose serious challenges for all sectors of the government and economy.

In testimony before the U.S. House Appropriations Subcommittee on Defense in May 2021, U.S. Space Force Chief of Space Operations Gen. John "Jay" Raymond said the nation needs to be concerned about efforts by Russia and China to disrupt capabilities in space.

"There is an active threat in the domain," he warned.

Meanwhile, Russia ramped up its efforts on the conventional front, mounting a brazen invasion of Ukraine on Feb. 24, 2022. The ultimate intentions of Russian President Vladimir Putin re-

main unclear, but much of the country has been devastated by constant bombing and missile attacks. The United States and its allies have since struggled with how to respond, with fears of nuclear war, conflict in space and cyber attacks looming on the horizon.

CHINA

China conducted two tests of newly developed hypersonic weapons on July 27 and Aug. 13, 2021. The Chinese government claimed the weapons can travel at least five times the speed of sound — 3,800 miles per hour — likely making them difficult to defend against.

"I don't know if it's quite a Sputnik moment, but I think it is very close to that," said Chairman of the Joint Chiefs of Staff Gen. Mark Milley. "It has all of our attention."

When it comes to efforts to militarize space, China could overtake the United States by 2030, according to Gen. Thompson.

"They are building and fielding and updating their space capabilities at twice the rate we are," he said at a Dec. 4, 2021, Reagan National Defense Forum panel discussion. "If we do not start accelerating our development and delivery capabilities, they will exceed us."

In addition, China is actively ramping up production of nuclear warheads, which military observers suggest could quadruple in number and reach 1,000 by 2030.

Estimates suggest that China has increased annual military spending by more than 6.8% this year, with a priority on securing its claim over the South China Sea where it is creating new islands as outposts. According to the Department of Defense, China now has the largest navy in the world, with about 355 ships and submarines ready for battle.

Throughout much of 2021, China military forces also encroached upon Taiwanese airspace to intimidate and expand its hold on the region. Over one four-day period in October 2021, approximately 150 Chinese aircraft flew inside Taiwan's defense zone.

With about 2,250 combat aircraft in its fleet, China now boasts the third largest air force on the globe. Its relatively new fifth-generation stealth fighter — the J-20 — was developed from technology likely stolen from U.S. firms and would be competitive with U.S. fighters.

> "[China is] building and fielding and updating their space capabilities at twice the rate we are. **If we do not start accelerating our development and delivery capabilities, they will exceed us."**
>
> **—Gen. David Thompson**
> Vice Chief of Space Operations, U.S. Space Force

But it is not all about military might. For years, China has also attacked the U.S. on the economic front. Some estimates suggests that China steals between $225 billion to $600 billion worth of intellectual property from U.S. firms every year. The thefts help China inch closer to its goal of dominating technological advances in the future, while seriously harming our overall national economy.

"They have gone from a peasant-based infantry army that was very, very large in 1979 to a very capable military that covers all the domains and has global ambitions," Gen. Milley said. "As we go forward — over the next 10, 20, 25 years — there is no question in my mind that the biggest geostrategic challenge to the United States is going to be China."

> **"Threats are more diverse, interconnected and viral than at any time in history.** Destruction can be invisible, latent and progressive."
>
> **—James Clapper**
> Former Director of National Intelligence

CYBER

In May 2021, cyber criminals hacked the Colonial Pipeline, which delivers nearly half of the East Coast's gasoline, jet fuel and diesel fuel. Forcing the company to shut down, the cyberattack had an immediate and stunning impact on the nation's economy.

Investigators later suggested that the DarkSide ransomware gang, which likely operates freely within Russia, was behind the cyberattack. In fact, most of the world's top ransomware offenders operate out of Russia.

According to the Cognyte Cyber Threat Intelligence Research Group, there were 1,112 ransomware attacks on global businesses and organizations in 2020. That number was expected to double by the end of 2021, costing firms millions of dollars in ransom payments.

More than half of all cyberattacks globally are against U.S. targets. In the first half of 2021 alone, the U.S. Treasury Department estimates over a half billion dollars in ransomware payouts were paid by those attacked.

Brig. Gen. (Ret.) Chris Inglis, national cyber director and USAFA Class of 1976, estimates that only 15% to 20% of all ransomware attacks and payments are officially reported. As a result, upwards of 80% of such mischief is not part of annual statistics for the ever-expanding crime.

Professional hackers continue to cause serious threats to networks on a daily basis. At risk, experts admit, are everything from the electrical power grid to the national banking system.

The New York Times, Wall Street Journal and Washington Post have all recently reported breaches in their computer systems. The Associated Press Twitter account was hacked, and a false tweet was posted, forcing the media organization to shut down its account to fix the problem.

China, thanks to support from its People's Liberation Army, is the world's number one country that harbors, pays or encourages cy-

ber criminals. Some estimate China's so-called "hacker army" numbers between 50,000 and 100,000 individuals. Other estimates suggest that about 40% of the world's unfriendly hackers reside there.

James Clapper, former director of national intelligence, called cyberattacks the top threat to national security.

"Threats are more diverse, interconnected and viral than at any time in history," he told Congress. "Destruction can be invisible, latent and progressive."

In his new national role, which has him officed at the White House and reporting regularly to President Joe Biden, Brig. Gen. (Ret.) Inglis says efforts are underway to get a handle on the true threat level of cyberattacks.

He says the nation has the tools necessary to defend itself in cyberspace, but it will take a more coordinated effort between the public and private sectors to be effective.

"The threats grow by the day," Inglis says, "but we're not actually doing the proper job necessary to actively defend those spaces."

He suggests that a cooperative approach — involving everyone from the Department of Defense to other federal agencies to private companies — is required to better protect the nation from attacks in the cyber realm. The nation, however, has a long way to advance before reaching that goal.

"Cyber is an inherently team sport," Inglis says. "The challenge is that we're largely stovepiped. They're independent of one another. On most days, we're practicing what I would describe as division of effort."

INFORMATION WARFARE

Two United States Air Force Academy graduates — Capt. Jeffrey Baptist (Class of 2013) and Maj. Julian Gluck (Class of 2012) — recently published a piece in the *Journal of Strategic Security* highlighting the efforts of adversaries to sway the opinions of the American public in ways that foment division and strife.

From alleged Russian interference in recent presidential elections to the sowing of political discord on social media platforms, adversaries have tapped a new source for distributing propaganda that is far more effective than dropping paper leaflets behind enemy lines.

"Unfortunately, the new baseline for interstate conflict has been set," Baptist and Gluck wrote. "The information realm has almost limitless potential for disruption, disinformation and narrative

manipulation. The free flow of ideas, Western democracy's civic bulwark, has become a wall both subverted and co-opted by actors veiled with plausible deniability."

As an example, Russia attempted to take full advantage of disinformation and misinformation during the early days of its Ukraine invasion. Russia's state-run media has flooded channels with lies to sway public opinion at home and around the globe.

According to Lt. Col. Chris "Fuego" Gausepohl, director of the Strategy and Warfare Center (SWC) and USAFA Class of 2005 graduate, disinformation and misinformation are powerful warfighting tools that adversaries can implement cheaply.

"Nobody thinks they are being misled," Gausepohl says, "but we see through a foggy lens with information pollution that is built up through our social media, our news and our day-to-day interactions with people. We're trying to inoculate DoD personnel against the misinformation/disinformation problem set."

ELECTRONIC WARFARE

Capabilities in electronic warfare — the disruption of information flow to help carry out intelligence and military missions — have increased dramatically among our adversaries. Today, the U.S. military relies heavily on connectivity to plan and execute missions. Any forced disruption in the ability to communicate can have disastrous results.

"We're in a race for military superiority, largely through technology," Secretary Kendall explains.

He says adversaries, such as China and Russia, have been building systems that are increasingly capable of targeting essential assets used by the United States.

"The information realm has almost limitless potential for disruption, disinformation and narrative manipulation. The free flow of ideas, Western democracy's civic bulwark, has become a wall both subverted and co-opted by actors veiled with plausible deniability."

Excerpt from *The Gray Legion: Information Warfare Within Our Gates*, by Capt. Jeffrey Baptist, U.S. Air Force information operations officer, and Maj. Julian Gluck, U.S. Air Force bomber instructor pilot.

Jamming capabilities targeting radar and radio communications are being perfected by Great Power competitors and likely will play a key role in the success of future conflicts.

Russia has used jamming efforts to great effect during its Ukraine invasion. The efforts were thwarted, to some extent, by Starlink's willingness to donate thousands of transmitters to bolster communications within the country. When hackers attempted to take down Starlink capabilities, the company was able to quickly defend against the attack.

According to Brig. Gen. Tad Clark, director of the Air Force's Electromagnetic Spectrum Superiority Directorate and USAFA Class of 1996 graduate, successfully operating in the electronic spectrum is key for maintaining our nation's air and space superiority. The cooperation of commercial partners, such as Starlink, improves the nation's chance for success, he adds.

"It's going to take a whole-of-nation approach to achieve the desired end state," he says. "The desired end state is not to go to war. But if we are called upon to go to war, then we need to

be able to access and move freely and offensively in the electromagnetic spectrum."

If the U.S. does not achieve superiority in the electromagnetic spectrum, Clark explains, the military can't communicate, use its radars, pass data, nor fly where they want to. Also, weapon systems that rely on GPS won't be able to find their target.

"Then we come to a grinding halt," he says. "And we can't do what we need to do."

FUTURE CONFLICT

"Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur." ***—Giulio Douhet***

It's a well-rehearsed quotation Air Force Academy cadets memorize from their copy of "Contrails" — a book of common knowledge issued to each student.

The United States Air Force Academy is taking that challenge to heart with new initiatives to better prepare cadets for the future and yet-to-be-defined fight.

"The future these cadets are going to inherit will be dramatically different from anything that I or my predecessors faced when they came into active duty," admits Col. Thomas Swaim, permanent professor and head of the Department of Military and Strategic Studies. "They're going to be facing a highly adaptable, technologically advanced, near-peer competitor that is well prepared to counter us on every front. These cadets will hit the ground running … ready to think innovatively and creatively."

To better anticipate that future, the Air Force Academy is ramping up several academic opportunities to equip cadets with the skills required to succeed in the air, space and cyber domains as military officers.

A CADET TRIES OUT THE NEW MULTI-DOMAIN LAB AT THE AIR FORCE ACADEMY.

- The Strategy and Warfare Center (SWC) is a research and experiential learning organization that launched in early 2020. According to Kyleanne Hunter, former SWC director, the SWC focuses on the future joint and multi-domain fight through research and projects that address real Air Force and Space Force challenges. "We do not do research in hopes that it will be policy relevant," Hunter says. "We do the work that is answering very concrete questions."

- A new Multi-Domain Laboratory, as part of the SWC initiative, was christened in September 2021. The $9.5 million facility housed in Fairchild Hall allows cadets to practice the various aspects of the future fight through interconnected simulators and immersive learning devices in a lab setting. "This space is one of a kind," Lt. Col. Gausepohl said. "For those of us who grew up in a classroom with four walls and an overhead projector or a whiteboard in the front, this changes learning. We cover cyber, space, air and sea inside this laboratory."

- The Institute for Future Conflict (IFC) was conceived and strongly endorsed by USAFA graduates who recognized the need for the U.S. to step up its game in order to stay competitive with the likes of Russia and China. In 2016, Dr. Paul Kaminski (USAFA Class of 1964), one of the key leaders in the development of stealth technology, hatched "The Big Idea," which eventually led to the establishment of the IFC.

  The Big Idea consisted of three major points:

1. Anticipate, rather than react to, changes.

2. Contribute to the next military offset. The success enjoyed by the U.S., and its allies and partners, during the Cold War was enabled by significant, technology-based capabilities that imposed unaffordable costs on our adversaries' ability to gain military advantage over the U.S. and its allies. The first offset was defined by multiple intercontinental delivery options for an overwhelming force of nuclear weapons. The second offset was defined by counterweighing larger forces with superior training and the integration of air and space sensors to provide global battlespace awareness, precision-guided munitions and the development of stealth technology. The next military offset will be driven by Fourth Industrial Revolution technologies, which will be different and will move faster than prior technological revolutions. For the first time since World War II and the launch of Sputnik, the U.S. finds itself lagging behind its potential adversaries in the key technology areas articulated in the National Defense Strategy.

3. Expose Air Force Academy cadets and permanent party to organizations and ideas shaping the future fight. Every commissioned graduate will serve in the profession of arms, and many will serve in leadership positions that will shape U.S. national security strategy, policy, capability and posture. The Academy's distinctive, immersive experience creates opportunity for holistic development of future officers not possible from other commissioning sources — the essence of the Long Blue Line.

> **"For the first time since World War II and the launch of Sputnik, the U.S. finds itself lagging behind its potential adversaries in the key technology areas articulated in the National Defense Strategy.**

Implementing the IFC

With Gen. Shwedo at the helm as its first director, the IFC is involving cadets in actively preparing for future conflict in all the emerging warfighting domains — cyber, space, artificial intelligence, hypersonics and more.

The IFC's objective is to provide the cadets and USAFA cadre with the insights and tools to better anticipate and drive change in the

character of 21st century conflict. And as Gen. Shwedo states, "it is planting the seed throughout the Cadet Wing that the key to our nation's future military success lies in joint and synergistic efforts."

"I want to open up the aperture so that throughout their career they are looking at multiple ways to attack a problem that always increase dilemmas for the adversary," Shwedo says, "and convince them that any conflict with the United States is not in their vested interests."

Today, the IFC conducts a weekly update brief to cadets and faculty that includes the latest developments in technology, conflict and geopolitical events. Lately, these briefs have focused on the war in Ukraine and its early lessons for future conflict.

Given the high stakes, it is no wonder the Institute for Future Conflict is one of the central priorities of the Air Force Academy Foundation's Defining Our Future campaign in support of the Academy's strategic plan.

In coordination with the IFC, USAFA also formed the Future Conflict Curriculum Review (FCCR) Committee. It was tasked to lead a limited review of the Academy's academic curriculum, to answer two questions:

1. How are we educating cadets to succeed in an ambiguous and rapidly changing world?

2. How does our academic curriculum prepare cadets to exploit emerging trends shaping future conflict, based on foundational Department of Defense guidance?

This comprehensive level of assessment of the academic curriculum explored how USAFA was preparing cadets for future conflict. While the report highlighted numerous strengths across the course of instruction, it also identified gaps in the curriculum and will drive change that will better prepare cadets for the future fight.

In addition, the dean of the faculty directed the development of a Scholar's "Z" Course, an interdisciplinary course incorporating law and computer science disciplines with an emphasis on integrating artificial intelligence. This course is intended to fill a gap identified in the FCCR of promoting interdisciplinary work.

The construction of the Madera Cyber Innovation Center is another opportunity that provides cadets with the ability to expand their exposure to emerging technologies and important future conflict topics. Once completed, the facility will bring cadets, military experts and industry officials together to collaborate on the challenging issues related to cybersecurity.

At the groundbreaking ceremony in August 2021, Paul Madera (Class of 1978) said the center is needed to prepare cadets for leadership in the current and future cyber battle.

"The reality of our world and the need for this cyber center for innovation resonated so clearly from the start," he said. "I have seen from the front lines, as an early-stage technology investor in Silicon Valley, just how difficult cybersecurity is. It is so very clear that every conflict we will face will involve cyber intrusions and attacks."

CONCLUSION

It does not take a prestigious think tank to envision what might happen to our nation's competitive advantage in the coming decades if things do not dramatically change in the near and long term. It comes down to "Accelerate Change or Lose," as the Air Force chief says.

That is why significant investment today in the tools and skills needed for the future fight can pay huge dividends for the U.S. and its allies when conflict arises. Left unchecked, near-peer competitors will continue to test the boundaries of our resolve as a nation. It would be foolish to let them continue to challenge us without enacting appropriate consequences and instituting effective defenses.

KEY TAKEAWAYS

- The "Accelerate Change or Lose" priorities will require continued investment in the preparation of our future military leaders for future conflict.
- Getting ready for future conflict requires a shift from reactive to proactive action.
- Success in future conflicts is a no-fail mission. Our nation's political and economic future depend on the proactive steps we take today.

DEFINING OUR FUTURE

THE CAMPAIGN IN SUPPORT OF
THE UNITED STATES AIR FORCE ACADEMY