Center for Strategic and International Studies

TRANSCRIPT

Event

Conflict in Focus

Air and Space Domain Lessons from Russia-Ukraine: Part One

DATE

Thursday, March 20, 2025 at 10:00 a.m. ET

FEATURING

Austin Gray

Co-founder, Blue Water Autonomy

Major General Gregory Gagnon

Deputy Chief of Space Operations for Intelligence, U.S. Space Force

CSIS EXPERTS

Matthew Slusher

Military Fellow, Defense and Security Department, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Mathew Slusher: Over the past three years of conflict, modern warfare has undergone a remarkable transformation. Welcome to part one of the Air and Space Domain, a special two-part episode of our series Conflict in Focus: Lessons from Russia-Ukraine.

(Music plays.)

I'm Colonel Matthew Slusher, a military Fellow at CSIS. And joining me today are esteemed experts who will offer in-depth analysis into critical lessons emerging from the ongoing war in Ukraine. Our first guest is Austin Gray. Austin previously served as an intelligence officer in the United States Navy. After that, he spent some time working on drone development inside Ukraine. He is now the cofounder of Blue Water Autonomy. Welcome, Austin, and thank you for being here.

Austin Gray: Thank you, Colonel Slusher. Excited for this conversation.

Col. Slusher So I've read over your bio and, man, what a list of accomplishments and experiences so far. And you've got a long ways to go, hopefully. Could you tell us a bit about your background and your journey to build autonomous vehicles?

Mr. Gray: Yeah, yeah. Thank you very much for the brief intro. And so I got started in the Navy as an intel officer. And I did something, I think, different than most junior officers in the intelligence corps do. And I started on the tech side. So I started doing IT on the classified systems for the Navy. And we got to do the basic maintenance of IT, and put new tech into the Pentagon – like, some of the first iPads and Microsoft Surface Pros. So I had that sort of grounding in the bureaucracy of how things are bought and how we field new tech.

And then I went out to the fleet, to aircraft carriers. Got to manage the top secret battle map for a couple different admirals, and kind of put the pieces together of where our ships – you know, how are we hunting the adverse submarines – adversary submarines, and then where are all the different capabilities that we have and that they have. Did a couple tours there. It was an amazing experience. And then got out, hit MIT's MBA program on the G.I. Bill. And then I did something a little bit different when I wrapped up with business school.

And, like you said, I went to Ukraine and I worked in a drone factory. And that just got me thinking so much about how fast this tech is moving, because they were updating the tech every single night software-wise, and updating the hardware often in a couple weeks cycle to get new systems to the guys on the front line. And so I spent a lot of time talking to the soldiers about what they were seeing and what they

needed, and then building supply chains so that they could build faster and build with ready components.

So I think that's a good launching point for us. And I took those lessons, and I started a company that's building autonomous ships. But I think I'm just excited to talk about the, you know, lessons from the air domain and how those apply to the rest of the future force architecture with you today.

Col. Slusher: Great. That's fascinating. Well, yeah, let's jump right into it. How critical of a role would you say autonomous vehicles has played thus far in the Russia-Ukraine war? And how has autonomous vehicles changed modern warfare?

Mr. Gray: Yeah. So it's – I mean, the reason we're talking, right, is it's massive. And so I think that – kind of like you and I were talking about right before this – there's sort of three things that I would walk us through as a framework. One is the high-level takeaway. Two is, where's the tech and the supply chain, what you can actually build quickly? And then, three, what matchups does that create on the battlefield for soldiers and airmen who are in the fight?

And so the high-level takeaway is, if you or I are in a foxhole doing our jobs, and we have a drone, we have a much longer range at which we can hit our adversary, right? So there's longer range. And we also can conduct that strike with much lower risk because we're not exposing ourselves, which is the most valuable things on the battlefield. And so then if we go to our commander and we say, hey, sir or ma'am, I can hit something at longer range and at lower risk because I have a drone, every commander everywhere is going to say: OK, that's longer range and lower risk. I like that every day of the week when I wake up. Right? And so that's what drones have done fundamentally I think is the high-level takeaway.

And so point two is the supply chain at the tech and, like, what can we do today. And it's hardware and software, right? And on the hardware side, the batteries are there. The basic lightweight compute is there. The materials to have airframes where you can just put something together that will fly on a small drone, it's all there.

We were ordering most of our parts and components for prototype testing and even for scaling sometimes in our factory in Ukraine from Amazon and Ali Baba because this stuff is commercially available off the shelf. Some of it you can 3-D print if you just have the right 3-D model. So the hardware is there.

The software, I think, is largely there too because you can control, from the firmware up to the operating system, most of those hardware pieces from pretty simple software. And if not, software cycle times mean you can just make it with a couple of the right engineers in your factory and everything is integrated together.

And there was a piece maybe two weeks ago from Harvard talking about you need full, like, dual-plated autonomy in the level-five autonomy. And, you know, maybe you need the – you know, the singularity to have a drone fly, you know, autonomously without humans controlling it. I don't think that's the right way to think about it. I think there's a lot you can do just with simple remote control and then with a little bit of autonomy that lets the drone work for a minute or two if there's not – you know, not perfect comms or there's some electronic interference. And then later we'll get to the full-autonomy thing. So the software is there too, I think, is the key takeaway.

And then point three is those matchups. And maybe we can talk through some of the graphics that you and I were looking at that show some of the matchups and how things are becoming attritable.

Col. Slusher: I think that's a great time to pull that up. Can we get chart one, please?

Mr. Gray: Yeah. So this is one of my favorites. And I think the thing I notice that I think got you and me talking originally, Matt, is when I went to the front line and got out there in their inside-artillery range, and I realized that everything around me on the front line was in the bottom left of this chart. And so this chart is set up with cheap things on the very far left and really expensive things on the right. And anyone can make a cheap-expensive graph. And almost everything DOD has would be on the far right.

But then I tried to create another axis where, whether it's really easy to target and destroy being on the bottom, and whether it's really challenging the target and destroy being on the very top. So something that has a lot of really good defenses or is very tough or is very stealthy would end up on the top, and it's probably going to be expensive. So it ends up in the top right. And that's most of our force.

But everything on the front line in Ukraine, almost everything, is in the bottom left, because it's really cheap. It's what we're calling a(n) attritable now, and it's stuff that – it can be hit, but maybe it's not worth hitting. And so the attritable things are having a lot of value.

But what I started thinking about is, well, that explains why drones are good and it explains why the Russians will just throw infantry into an

assault, because they don't value their infantry like we do. And it explains a lot of what's going on. But it doesn't really explain, you know, how some of the vehicles might still be effective, how the collaborative combat aircraft might still be effective, because you can see those, you know, tanks and CCA and maybe Special Forces and unmanned warships kind of in the middle here.

And in the middle – you know, it just doesn't really explain why they're – why they're useful, because most of the force is on the bottom left or on the top right. And, of course, you have the bottom right, which is stuff that's dead, right – some of the big ships; I think in the air domain some of our Global War on Terror era UAFs, the $100 million unmanned aerial systems with low-stealth, easy to shoot, no defenses, those pop up there.

So maybe we can go to the next – the next chart and talk more about some of those things in the middle, tanks and, you know, collaborative combat aircraft and why the matchup works out well.

Col. Slusher: Yeah.

Mr. Gray: And so this one is exciting. So here what I started thinking about is, all right, well, if you have a – if you have a fighter jet, fighter bomber right on top, and say we're the Russians, right? Say that's a Su-35 going on a strike mission. Well, if it's going on a strike mission, if it's facing the first thing on this – on this graphic, an infantry unit, obviously, the fighter bomber can hit an infantry unit. If it's facing the next thing, it's a vehicle; it can probably hit it too.

Once it faces some air defenses, like that missile system, the third one, then it's facing some risk, right? And suddenly you have a $100 million plane matched up against a – against a missile battery. You have some risk. And if you're going to try to strike, you know, the adversary's command center with really good air defenses, that's a lot of risk.

And so if it's worth hitting it, fine; go for it. But don't take on – don't take on too much risk to make that – to make that strike. But if you start looking at what missiles and drones can do for you, they can do some of those same strikes with either zero risk or with just a lot less risk than the adversary would have by shooting at them, or cost if you're just going with the cost of your ammo, and so you can create match ups.

And so if we go to the next slide, or the next graph, excuse me, that brings you to a force architecture where you don't just have the expendable stuff on the bottom left and the survival stuff on the top right. You have this force architecture with kind of a nice continuum

where you have your expendable assets, you have attritable, you have things you can risk but don't really want to get rid of, and then you have the survivable.

And so I think we're moving into a – we're moving into a force architecture where you kind of have to have capability across all parts of the spectrum so that you could always have a favorable matchup with the adversary or guarantee that they can have a really unfavorable matchup against you.

Col. Slusher: That's great.

Next question. What would you say are the most significant vulnerabilities or risks of using autonomous drones in warfare, both for the operators and for the targets?

Mr. Gray: So I think that the thing that jumps out for the operators is that if you're still doing a remote control drone, if you're the operator and you're flying the drone from your command bunker it might be easier for me to find and take out you, the operator, than it is to take out that drone because the drone is a small target, right?

Col. Slusher: Yes.

Mr. Gray: And you probably have a central node. So that's one of them.

And I think the other one that really sharp people draw attention to all the time is just the cybersecurity risk and the electronic interference risk. You've got to create platforms that are – sure, they're cheap. You can build them quickly.

But they're tough enough and smart enough to not let the adversary trick them, you know, with hacking or with EW or with any other sort of decoy operation because they don't necessarily have humans there making decisions for them and the machines are thinking for themselves a little bit. So I think the cybersecurity is pretty important too.

Col. Slusher: Do you find that distance is a factor in securing a link?

Mr. Gray: I think what we've seen is that in Ukraine distance has been mitigated by, one, satellite comms that can be nodes; two, by relay stations locally that are sometimes air breathing or sometimes ground based and create more resilient mesh networks.

And the original probably risk or concern over distance was, oh, well,

we won't be able to communicate once it goes with it – once it goes over the horizon. I think that's becoming less of a concern especially as we get towards a mesh network of, all right, well, now we've got five different nodes this thing can talk back to and it only needs to get to one of them, and the adversary might be able to jam a couple of them but they're probably unlikely to jam five at a time, you know, continuously. And guess what? If they jam five that's a lot of resources they're expending to do that and we'll just add a sixth.

Col. Slusher: That's great.

How do you see autonomous drones being used in future warfare scenarios and do you see any new types of mission sets or combat roles that they would fulfill?

Mr. Gray: Yes. So I think that autonomous drones are going to have to fit into that middle portion of the framework. We've had expendable and attritable assets for a long time. Expendable is just ammo, right? You use it once and that's it.

We've had infantry and sort of expensive ammo that's more attritable for a long time and then we're really good at building the big, survivable stuff – you know, ships and captain and expensive aircraft with pilots who trained their whole careers.

But the autonomous and semi-autonomous, things like the Collaborative Combat Aircraft or, like, a lot of the Navy's unmanned warships that they're thinking about, these $50 million unmanned surface vessels or unmanned submarines, those things are – they're expensive enough that you don't want to produce, you know, thousands of them but you can make some more if you lose them and you don't have the humans on there so it's acceptable to lose them.

And so I think that the autonomous platforms need to get smart enough and good enough that they can control the hardware to take on some of those riskier missions and then go hold the adversary's capital, warships, and command posts, et cetera, at risk.

And I think that's why the Collaborative Combat Aircraft is so exciting to me because it can work right alongside the manned fighter pilots and take on the riskiest parts of the mission.

Col. Slusher: Yeah. Total game changer. Tons of potential.

How will advancements in drone technology impact global security, especially in regards to smaller nonstate actors that want to gain access

to advanced drone systems?

Mr. Gray: Yeah. It's such a pressing question, Matt, because that's something that the U.S. forces are facing today, right? In real combat operations over the last six months U.S. Navy warships and aviators have come under fire from the Houthis in the Red Sea. The Russians, obviously, felt this pain in the Black Sea and on the front lines of the Donbas for a couple of years now.

But what we've observed is the Houthis can launch a strike with a thousand-dollar drone, or with a couple-thousand-dollar missile. Could be in the air, on the sea, or it doesn't really matter. And they can put at risk a billion-dollar warship, right? And we send up our F-18s or our F-35s to shoot these down in a cheaper manner, so we don't have to burn million-dollar missiles.

But we just need to create matchups where the bad guys can't always have the asymmetry. And so I think we need to – we need to have some ways of building stuff cheaply ourselves and relying on the easy parts of the supply chain, not always going to the really hard, really expensive, you know, over requirements, over-specced, you know, parts of the supply chain. Because we can build stuff cheap too. We're good at building. We're good at building new tech here in the United States. And look at what SpaceX has done disaggregating the satellite constellations. I think that's happening the air right now with a lot of smaller drones. I think it can happen on the ground and on the surface of the water too pretty soon.

Col. Slusher: Do you think there's a culture shift in the defense industrial base to where now the defense industries may feel like they're ready to have the support of the government to provide and produce these types of things?

Mr. Gray: I think there is some cultural shift already in the defense industrial base. Partially from new entrants, like from tech companies. Partially from slight cultural shifts in some of the bigger defense primes. But I think the cultural shift that we're still really waiting for is in the acquisition corps and the requirements corps in the Pentagon. And they've got some work to do. I think the new administration's working on it. But they've got to just get used to taking some risk and, you know, buying a couple of different drones, right?

And say my drone company and your drone company and a few others are making the CCA, or whatever it is, doing a portfolio approach and taking some bets. And the competition between us, I think, will flush out, all right, well, Matt's got the best – he's got the best he's got the best

drone in his company, so we're going to go forward with that one, and produce a bunch of those. And that would probably be a cheaper strategy over the long term.

Col. Slusher: Yeah. Let's hope for that. All right, we have time for one final question here. What technological advancements do you predict may shape the future of drones in warfare, say, over the next 10 to 20 years?

Mr. Gray: It's a really interesting one. I think we talked a little bit about, you know, the singularity and where is autonomy going. I think that's just a gradual scale of, OK, we're moving up that scale from remotely controlled all the way up towards fully autonomous. The other one that I think is happening a little bit, but it won't be the real breakthrough that we're looking for, is the EW space. There's a lot of really well-deserved attention paid to the electronic warfare space. But we've seen that, despite all the electronic warfare, all the jamming, all the deception, drones still fly, missiles still hit their targets most of the time, because you can innovate and get around – you can have spectrum maneuver and get around a lot of the – a lot of the jamming that's going on. Be it from using other parts of the spectrum, using a tether, or just having a resilient comms network.

So I would say that the EW space is one where having comms and assured command and control will be more likely to keep occurring than some sort of crazy breakthrough. But the place I would look for more innovation would probably just be in how do we link hardware and software better and have software control our hardware and have software-centric systems? I think the tech is there. And it's much more about applying it now and building our contracts around incentivizing people to build the right tech.

Col. Slusher: Awesome. Well, do you have any closing comments?

Mr. Gray: No, this has been great. I mean, you guys have put on such a – I think, a great event around discussing some of the most important trends in the industry. And the air domain is leading the way in unmanned systems. And, for my sake, I hope the maritime domain, and the undersea domain, and everybody else catches up and keeps solving the hard problems.

Col. Slusher: Yeah. Well, this has been great on my end. You know, thank you so much for sharing your time and perspective. And I deeply wish you continued success in your already brilliant career. So thank you.

Mr. Gray: Thank you, Matt. Same to you.

Col. Slusher: Our next guest is Major General Gregory Gagnon, United States Space Force. He's the deputy chief of space operations for intelligence, responsible to the secretary of the Air Force, and chief of space operations for policy, oversight, and guidance of Space Force intelligence operations and production.

General, it's an honor to have you with us today. Thank you so much for being here.

Major General Gregory Gagnon: Oh, it's my pleasure. Thanks for the topic. And I look forward to our discussion.

Col. Slusher: Thank you. Well, if it's OK we'll just jump right into it then. First question, General. Russia has heavily focused on influencing the information space, with one notable example being the Viasat cyberattack. Can you discuss the implications of this attack on space assets, and how it reflects on the broader challenges in securing the information space?

Maj. Gen. Gagnon: Yeah. As we set those activities, we should set those activities with regard to time and with regard to the crisis. So, for the second Russian invasion of Ukraine – which, of course, was about three years ago in February – there was activities that predated what we saw militarily along that border line. The information space became incredibly important in that conflict. It became important in that conflict in how we told our story as a nation, that we expected Russia would conduct a second invasion deep into Ukraine. It became important in how we gained partners across the Atlantic. And it became important in how we battled other narratives for truth. Both cyberspace and space played a key role in that.

You highlighted, first, the Viasat attack by the Russians, and what I would like to highlight for the group is that this is a long-held tactic that goes back to Soviet times. In Soviet doctrine and in early Russian doctrine, they have a concept known as information confrontation. Information confrontation has two subsets. It has information technical and information political. The information technical is how you use technical assets such as electronic warfare assets or cyberspace assets to control the means of disseminations of the message. The information political is the part that is the message itself. And of course, you know, Putin and those before him have always had to do propaganda domestically to maintain their leadership position in that society because they're not really elected, and in those events they become experts at propaganda to their own domestic population.

Information confrontation is a power-projecting capability to use propaganda or that political warfare in a way that helps achieve military objectives. The Viasat attack is an example of that. The actual technical attack is information confrontation technical. It was where they seeked to disrupt the Ukrainian military command-and-control capability. And in launching that attack – and the timing is important; it happened just before the start of the war, on I think the 22nd or the 23rd of February. And in doing so, they were attempting to do command-and-control warfare.

But their impacts were not the impacts they expected. They were unable to disrupt the Ukrainian military command and control. And in fact, they had effects that broadly hit large parts of Europe, if you read the open source. So 5,800 wind turbines were disconnected from their remote controllers that went back to the German electric and power companies. There was satellite internet disruption to about 9,000 French subscribers. And then secondary internet service providers also felt impacts of about 13,000 subscribers across Europe. So they executed it because it was a key objective in the start of their war. And one of the lessons, I think, we draw from this is that gaining cyber and space superiority over your asset – adversaries is an early objective in ground campaigns. And I think that will play out as we move forward later into the 21st century with additional conflict.

Col. Slusher: Absolutely.

Despite Russia's significant military capabilities, they have struggled to effectively use space for combined arms employment. What do you think were the key factors that hindered Russia's ability to integrate space operations into their overall military strategy?

Maj. Gen. Gagnon: Yeah. So most people, when they want to put a yardstick out and measure how a military performs, they reach into their closet and they pull out a yardstick, OK? And that yardstick is the American military way of war, right? And you start to measure them against that.

For the American military way of war, there are two things that are very important.

One is space control or what we call space superiority, the ability to use space at the time and place of your choosing and deny that to your adversaries. When you pull out the American yardstick and try to measure people, most people don't have the capabilities that the United States have. So they have to, one, seize the opportunity to gain and exploit space superiority.

The second part of that yardstick is the American way of war is fueled by controlling the high ground, whether that high ground is outer space or that high ground is airspace, OK? Russia failed to achieve both of those objectives early in the war, and to this day remains contested against the Ukrainians.

In outer space, you would say: How could they not achieve space superiority, General Gagnon? That makes no sense. The Ukrainians don't really have a space force. But what was in outer space was a series of remote sensors from commercial companies that were leveraged by dollars from Europe and dollars from the United States to help expose what the Russians were trying to do and provide remote sensing and intelligence to the Ukrainian force. The Russians were unable to compete at that scale. That was in space.

In the airspace domain, neither country has been able to gain air superiority over the battlefield. And the lack of space superiority and air superiority has turned what we are seeing in Ukraine to look a lot like what we saw in World War I. It's a stalemate, trench warfare. And if you measure the Russian military against that, against that American way of war, they got an F-minus. And I'll give you one other thing. And this is why we can do the American way of war, OK? The Russian military is 11 percent conscripted. They're conscripted for a year. The Russian military lacks a professional NCO Corps.

If you want to conduct combined arms – that's operations from space forces, air forces, ground forces and maritime forces – and you want them to act as a unified whole, you have to communicate, coordinate, and empower at low levels. U.S. military officers set the stage and the context for that type of behavior, but that type of behavior inside our fighting formations is carried out by a professional NCO Corps. The reason the American yardstick is the largest yardstick in the world is because of our NCO Corps.

Col. Slusher: That's a great point. And really, nobody can compete. We've got the gold standard on that. Switching to electromagnetic spectrum. This plays a crucial –

Maj. Gen. Gagnon: You're getting real nerdy with people now, so OK.

Col. Slusher: Yeah. Bear with me. It'll only get worse from here. (Laughter.) It has played a crucial role in modern warfare, as we've see this conflict play out. Can you explain why it's so critical for military operations, particularly in space? And what challenges arise in trying to secure and manage that spectrum?

Maj. Gen. Gagnon: Yeah. The electromagnetic spectrum is absolutely critical to long-range fires, the ability to strike things at a great distance. If they're fixed, or even more so if those targets are mobile. Because if that target is mobile and it's at great distance, you need to track that target. You need to find where that target is, and where it's headed, and where it'll be at a point of time so that you can fire a long-range weapon to have weapon effects. In order to do that, you're usually dealing with a satellite or an UAV and a ground firing unit or an air firing unit. You have to network together that force. That type of network happens through the electromagnetic spectrum.

That electromagnetic spectrum, if you do not have access to it, to use it uninhibited or work through it when it is disrupted, you cannot bring your network to bear. That's what makes U.S. fighting forces so effective. Twenty-five years ago there was a concept in D.C. from the late Admiral Cebrowski, which was called network-centric warfare. It was how to link your sensors to your decision makers and to your shooters. That's the concept that fueled the U.S. Department of Defense for 20 years as we pursued Joint Vision 2020. And I find it funny today, because 2020 was five years ago, but that is the underlying principle of how our unified force fights from a technology perspective. And it is critically dependent on the electromagnetic spectrum.

One of our challenges in the Department of Defense is that we started to undervalue how important it was to have spectrum superiority. And that's because we had 20 years of fighting in the Middle East against adversaries who are not challenging our spectrum use. Those core skills, which will be resident in some select officers and really our NCO Corps, are the special sauce that allow us to project power in a unified manner against both fixed and mobile targets.

Col. Slusher: Absolutely. It's hard enough to find, fix, track, and target time-sensitive things when you're not challenged in that spectrum. We've seen Russia increase its on-orbit activity in space, particularly with the launch of more sensing satellites. How do these developments impact our space security? And what does this mean for the future of space operations?

Maj. Gen. Gagnon: Yeah. So let me kind of address that in two ways. How does it affect our ability to use space to our advantage?

First off, the Russians are rapidly weaponizing outer space with both assets in the domain – such as satellites that, like a Matryoshka doll, they send out another sub-satellite that is really a weapon in space. And they first did that in 2019 and then, I think, in 2021 again. And they've

continued those programs because they are trying to hold at risk how the great U.S. military can use outer space, but not just holding our capabilities at risk.

They also seek to use outer space so that they can be more effective on the ground. Going into this conflict, their capabilities in outer space were unable to be brought to bear into their find, fix, target, tracking, gauge, assess cycle, which is the American way of framing how we put that network together that I talked about.

If you're in the Russian doctrine, you would call that the reconnaissance strike complex. And they call that the sensors that link to the command-and-control elements that link to the shooter. So it's the same concept, different name. They were unable to bring it to bear because those assets resided in different organizations. And the Russian military – one of the things we learned from this war is just how siloed they were and how much there was a lack of trust across these siloes to help bring to bear the full capability of the Red Army.

The Red Army, going into this war, was the third-most-powerful army in the world conventionally and the second-most-powerful nuclear power in the world. We did not expect them to perform so poorly. They performed poorly because they do not have a professional NCO corps. They lack trust internally. And that impacted their performance on the battlefield.

Col. Slusher: Great observations.

There have been reports of a growing nexus between China and Russia, with Chinese companies such as Space City, for example, providing commercial imagery to support Russian operations. What are the security implications of this partnership? And how do you think that's going to affect the balance of power in space?

Maj. Gen. Gagnon: Yeah. So to be honest, you know, as the head of an intel element, I get to read the most classified newspaper every day. So I'm not surprised that often. I was surprised when we saw this reversal in the relationship between the Russians and the Chinese and that the Russians needed to go to the Chinese to help them achieve reconnaissance from outer space, even commercially, right. That was a little bit of a surprise because, going into this war, Russia had a little bit under 200 satellites in outer space. Today they have just under 300. So they have spent the last 12 to 16 months really adding to their remote sensing in outer space, trying to solve one of their deficiencies.

But that relationship, where the second-most-important space country

wasn't Russia, it was China, and from remote sensing, they were leveraging commercial remote sensing from the Chinese private sector, was actually slightly surprising to me. But this is only the tip of the iceberg in the relationship, which is also very concerning.

Before the war, nobody would think that the Iranians would send weapons to the Russians to use in war. Nobody would think that North Korean soldiers would leave North Korea and go to Russia to fight in the war. Nobody would think that the lifeline economically for Russia would become China, OK. Many things have changed in three years that most people don't really remember, because three years went by pretty fast. But in February 2022, we had the no-limits declaration from both President Putin and Chairman Xi, right. And it was before the Olympics. So most of us were excited, waiting for the Olympics, not sure what this was all about. But that no-limits declaration was their statement before President Putin reinvaded Ukraine.

Since that time, the second thing that has really occurred is an acceleration in the combined training of their two militaries. So today Russian military forces and Chinese PLA military forces practice and rehearse together. They do it in ground exercises in either of the two countries, generally between eight and 10 times a year. And they've done that for a number of years.

What's new is we've seen cooperative maritime-vessel deployments that have circumnavigated around Japan in the last two years. And we've also seen combined-bomber exercises and drills between the bomber forces of the Russian military and the bomber forces of the PLA. So they are definitely working together at a military level with the desired goal of messaging Washington, D.C. that they could be a partnership if either one was put at risk.

The third thing I will tell you is the economic integration has been profound and tremendously different than what we had before the war. Increasing trade relations between Russia and China – in 2023 those trade relations went up 43 percent. One of the key goods of trade is, of course, oil and gas from Russia to China. That allows China to send money to Russia.

That money that is sent to Russia can then be used for buying up microelectronics for the Russian government and the Russian economy. Ninety percent of the microelectronics for Russia come from China. Of course, most microelectronics that would come from the West or come from the United States are on sanction lists so we can't send them there.

So this new global economy where the second largest economy in the

world is the Chinese is creating new dynamic relationships between Moscow and Beijing. I'm just hitting the tip of the iceberg on this, but they are growing closer together. They want us to believe that they are partners with no limits. But I also know that history tells us they're not partners with no limits.

Col. Slusher: Thank you for that, sir.

On the lessons learned train, what would you say if you could choose, like, an ultimate lesson learned or a key takeaway for, you know, any world leader that might be tuning in to watch our episode or anyone at home who's been watching this conflict play out? What would you say is just the – one of the biggest takeaways from the whole thing?

Maj. Gen. Gagnon: I would say that for conventional formations, like what we saw in the buildup for Desert Storm I – which is kind of me going back to Cadet Gagnon times – or what we saw with the second Russian invasion into Ukraine, that buildup of conventional forces where we can count how many BTGs the Russians have put together.

One of the big lessons out of this war is that – is really the loss of surprise for conventional forces. Large mass conventional forces will have a hard time executing surprise in the future and let me explain why.

As that activity was taking place and those forces were building up east of Ukraine commercial imaging companies in Europe and in the United States were putting out images. They were being run in newspapers and in journals and in think tanks, and think tanks were literally counting the number of Russian forces on the border.

It's hard to mask conventional forces, I think, in the future in a way that isn't going to be observed because the commercial remote sensing market in outer space is becoming rapidly an unblinking eye.

Now, that has implications for those autocratic regimes who look to expand their territory often – you know, always at the expense of their neighbors and, you know, a world that respects borders is a world that benefits the United States.

So maybe this commercial unblinking eye from outer space is in fact a benefit to the United States.

Col. Slusher: I think so. Still got time for a couple more here.

How do you assess the evolving challenges in the space domain,

particularly in terms of strategic deterrence, defense, and asset protection?

Maj. Gen. Gagnon: I was really excited that you asked this question and I really think it's three different questions.

But the first thing I wanted to talk about – and CSIS publishes stuff on deterrence regularly as do the other think tanks in town – deterrence isn't domain specific. We continue to misuse Schelling in amazing ways. But deterrence takes place in an adversary decision maker's head. It happens in these six inches, right?

You will use all elements of power. You will use diplomatic elements of power. You'll use those information elements of power. Maybe it's information confrontation if you're the Russians, right? You will try to erode support in that country you're trying to attack, right? That is one of their things.

Maybe it's a military instrument of power by moving forces – conventional forces – so that they can respond more rapidly or maybe you will use sanctions and economic and financial instruments to shape someone's decision making.

So when they talk about space deterrence I don't believe in space deterrence. I believe in deterrence. I believe in coercion. OK. These are specific terms for foreign policy experts. But you're simply trying to prevent an adversary from doing something or you're trying to get them to reverse something they did.

That takes place in all domains, and what you must do is understand what they hold dear because if you want to influence someone you must hold them at risk or hold what they value most at risk. I will tell you we have a benefit in the United States that our adversaries – whether it be North Korea, Iran, Moscow, or Beijing – they all have one thing in common. They're autocratic regimes that fear their people.

We believe in free and open access to information. We're helping democratize information around the world by building proliferated LEO architecture that allow internet on your phone anywhere. Those countries have to control their information environment so that they can control the propaganda to their people, so that they can continue to rule. This is their greatest fear. Their greatest fear is being removed from within. The future world is a world that's more connected. The statistics are clear. The world becomes a more difficult place for them, not a more difficult place for an open democracy.

Col. Slusher: Let's hope so.

Sir, how is the U.S. Space Force preparing to counter adversaries who are rapidly developing antisatellite capabilities and other space-related threats?

Maj. Gen. Gagnon: Mmm hmm. We're doing more than just planning to do it. We're actually already begun doing it. So our adversaries, whether it be the Russian military, or the Chinese Communist Party armed wing known as the People's Liberation Army, right? Both have their space forces as well. They are both rapidly weaponizing outer space. They are weaponizing it by putting weapons in outer space. They are weaponizing it by developing and demonstrating capabilities from the ground to destroy satellites in outer space. We have seen this coming for six years. Seeing that coming is why we moved to more resilient architectures in outer space.

In the past, the model that you would use as an investment banker – OK, the Pentagon really is investment bankers, right, about military capability – is if I had a satellite in outer space, and I could have it in just the right spot, and I could put as much capability on it as I could, I would do that because the cost of launching the outer space was so high. But I'd only have, like, one of them. So it would really be a critical node.

Moving forward for Department of Defense capabilities – whether it be global missile warning, that is growing to global missile track, which allows us to intercept, right? Or it's reconnaissance and surveillance from outer space so that we have an unblinking eye on our adversary. Or, let's say, it's secure communications for that ship to talk to that aircraft, or that U.S. aircraft to talk to a foreign partner. We have proliferated those architectures and have already begun the launch cadence to significantly increase the number of satellites in outer space.

For the U.S. national security enterprise, the Space Force will add over a hundred satellites just in 2025, which is a – which is a significant number. So we have studied it. We've planned it. And we're already started doing it. And that is to add resilient capabilities for our war-winning capabilities. Missile warning and missile track. Secure communications for the force. And, of course, reconnaissance and sensing that allows us to close long-range fires on a scale that no other country can really be. Now, that's part of what we're doing.

The second part of what we're doing is we're protecting and defending those assets. Our adversaries seek to extend war to outer space. We don't. But we know that we must be prepared for war in outer space.

Which is why this country, five years ago, established a military service known as the United States Space Force. We must protect and defend our assets. And we must be able to hold their assets at risk at the time and place and manner of our choosing as part of the joint force, so that the adversary can't use the outer space layer against our own forces.

I will tell you, it's not really the lesson from Russia, but a lesson from China is their rapid advancement in outer space from remote sensing. In 2022 and 2023, they added 200 satellites each year. Half of those satellites were remote sensing. They are attempting to create an unblinking eye in East Asia so that U.S. military forces cannot push west without being in what's known as a weapons engagement zone. We cannot allow that weapons engagement zone to stand if we are drawn into conflict and given orders from our political leadership to, you know, defend allies and partners. So the Space Force must be ready to protect and defend and, as part of the joint force, make sure that we can erode other countries' investments in space.

Col. Slusher: Well, sir, well, that takes us right up to our time. Did you have anything that you would like to close with?

Maj. Gen. Gagnon: I would like to pivot just slightly about sort of my opening comments to my closing comments. I've been in the military over 30 years. And when I started, when I was Cadet Gagnon, the United States military was quite large. The numbers are actually quite profound in the difference in, you know, numbers of soldiers at the Army had. They had about 732,000 when I was a cadet. They have 445,000 today. The United States Navy was a 600-ship navy. It's now a 300-ship navy. The United States Air Force had over 10,000 aircraft. Today, they got over 5,000 aircraft. All of these investments or divestments into the military services were made because we could control space. We could connect these platforms and make them more lethal. It was the principal thesis statement of network-centric warfare and Joint Force 2020.

Today, we're in a situation where if we were in a slugfest with another near-peer competitor – say, China or Russia – if we could not seize the high ground effectively, and the high ground is space, we should expect to see a war that looks like the Russia-Ukraine war. So we must make sure that we can gain and maintain space superiority because space superiority unlocks all the other key capabilities of our air forces, our ground forces and our maritime forces. That's why those forces can be 40 percent smaller today – which is 30 years later – but more lethal and more effective, because space superiority is greater than the sum of its parts. It must be invested in. It's a new mission for the Space Force. And the nation must make the decision to grow the Space Force to the size it needs so that space superiority is not in question.

Col. Slusher: Hundred percent, sir. So, I mean, fascinating and critical work that the Space Force is doing. I just want to thank you and your team for what you're doing for this nation. Thank you.

Maj. Gen. Gagnon: Thank you.

Col. Slusher: That wraps up part one. Please come back for part two of the Air and Space Domain Episode. Find this episode and more on YouTube and at CSIS.org. Thank you for watching.

(END.)