Masters of Scale: Rapid Response Transcript – Mike Brown

“Public-private opportunities, with Defense Innovation Unit's Mike Brown”

Click here to listen to the full Masters of Scale: Rapid Response episode with Mike Brown.

> **MIKE BROWN:** Artificial intelligence, biotechnology, autonomous systems, cybersecurity. We need a different way of doing business with the commercial world. That's what DIU is all about. How do we understand who the companies are that are developing those technologies, and how do we have a process that makes the Department of Defense as friendly as possible for those vendors?
>
> So the experiment is working. We've delivered 25 different capabilities now to the military that they didn't have before from commercial sources. We've introduced 65 first-time vendors to the Department of Defense. We have started our 100th project. We're doing twice as many projects as we did two years ago. We're seeing 100% increase year over year in terms of the company submissions to DIU.
>
> I'm proud of that track record that our DIU team is establishing, but relative to DOD, which has probably bought 1 trillion, 2 trillion, or 3 trillion dollars in that time period, we're a drop in the bucket. So I think that we've proven the benefit of how we work. There's a lot more commercial technology we could be taking advantage of. We need more emphasis on how we scale what DIU is doing to help the Department of Defense.

BOB SAFIAN: That’s Mike Brown, director of the Defense Innovation Unit within the U.S. Department of Defense.

Mike’s role is to help bridge the gap between technology innovators and the U.S. government, and during the Covid-19 crisis, he’s used that position to introduce some cutting edge projects that advanced the health safety of military personnel.

I’m Bob Safian, former editor of Fast Company, founder of The Flux Group, and host of Masters of Scale: Rapid Response.

I wanted to talk with Mike because, with so many health and other challenges facing the United States, public-private partnerships could be a key way to accelerate meeting those challenges. And no one has a more insider's view of the industry-government interchange than Mike. As the former CEO of Symantec, Mike experienced working with the government from the private side.

He knows that public private partnerships can be a big growth opportunity for businesses, and he’s become a key ambassador between Silicon Valley and Washington. He also has a keen eye on China’s tech efforts, and its potential impact on U.S. companies and U.S. national security.

Bringing the best of commercial tech into the government, Mike says, isn't just a nice to have, but a need to have.

[THEME MUSIC]

SAFIAN: I'm Bob Safian, and I'm here with Mike Brown, the director of the Defense Innovation Unit of the U.S. Department of Defense. Mike's coming to us from his home in Palo Alto, California as I ask my questions from my home in Brooklyn, New York. Mike, thanks for joining us.

> **BROWN:** Thanks for having me. Looking forward to the conversation, Bob.

SAFIAN: So before we dig in on your Rapid Response, I'd love to get some context from you. You were previously the CEO of Symantec. Before that, you're CEO of Quantum. You have a lot of experience in the private sector. Now, more recently you work in the public sector. These are two spheres that engage, but often don't really connect quite naturally. What's the difference between working in the corporate world and for the government?

> **BROWN:** Well, there's probably quite a few differences, but one that will immediately strike you if you join the government is the way Congress allocates money. I've heard it said that every government organization has 535 members of the board of directors – that's our Congress. Very different in terms of working with a corporate board, which actually provides a lot more flexibility for the CEO to pursue a strategy and working with the Congress, which would like to be informed about what's happening, has different "colors" of money, as they're called. So appropriations come not only by year and then by color – in terms of what you can spend for ongoing expenses, what you can spend for R&D. They all have different expiration points. Those are not fungible between categories.
>
> And you have a lot of folks who are interested in what your organization is doing. So for the defense innovation unit, being a part of the Department of Defense, we have House Armed Services committee, Senate Armed Services Committee, House Appropriations Committee, Subcommittee on Defense, and same thing on the Senate side. So you have four committees with congressional oversight. So it was a big difference in terms of your flexibility.

SAFIAN: Now your mission is to try to integrate more public-private partnerships. What are the things that private sector folks most misunderstand about working with the government?

> **BROWN:** Well, I'd say number one might be what we just discussed. Sometimes you're not able to move as quickly because of the different way funds are allocated. What we try and do is mask as much of that as possible so that we don't have to have every company that wants to work with us understand both the organization of the Department

of Defense, which is complex, the biggest organization in the world, and those details about how money is allocated and what authorities you're operating under, et cetera.

SAFIAN: All those rules, entrepreneurs don't really like rules a lot of the time, right?

BROWN: Exactly. They're motivated to move as fast as possible. So really, how do we reflect the opportunity costs that small innovative organizations have in working with Department of Defense? Of course, there's a well-developed routine for the large defense contractors who have a business model that is suited to working with what the Department of Defense requires. But we want to take advantage of all of the innovative capacity, the great things that are happening all across the country. So to do that, we've got to make sure that we have a process that's agile, is fast. So that's really what we've set up. And we have a special process, we call it commercial solutions opening that really makes it easy to interact with us and gets companies an answer quickly.

Even if that's a no, even if they're not going to be the vendor that's selected, as we all know, it's more important for companies to get that answer quickly than to waste a lot of time and find out later that they're not going to be moving forward. So we're all about speed.

SAFIAN: So the Defense Innovation Unit, which you run, it's relatively new. Five or six years old. Offices in Silicon Valley, Austin, DC, Boston. The goal is facilitating these public-private partnerships between the tech industry and the DOD. Heading into 2020, you had 50, 60, 70 projects underway, something like that. Then the pandemic hits. Now you had plans. All leaders have plans all the time. How did the changed environment impact those plans, the trajectory you thought you were going to be on versus where you ended up focusing your attention?

BROWN: Right. Well, maybe I can just also take a minute to provide a little more clarity on what public private-partnership means in this context. We are providing revenue contracts for small companies to first prototype their solution with the Department of Defense. And that doesn't mean a prototype in the sense that it's an immature technology. It might be a very mature technology in the commercial world. So we use that term to mean: just test it in the government environment. Test it in the real world military application.

And we want to make sure that we do that quickly. And that's one year if it's a software project, two years if it's a hardware project, to then get access for that company to production volume and contract dollars. So the Defense Innovation Unit really is all about getting companies access to the large contract dollars that DOD awards. So that's what we mean by a public private partnership there.

Your question about COVID, you're right. Like all organizations, we had to go through quite an adaptation. It really came in three flavors. One, can we operate when we're not all face-to-face in the office every day? Now the good news about our work at Defense

Innovation Unit is we were already set up on commercial tools. So we had it a lot easier than many of our brethren at the Pentagon who had to figure out, okay, how do we work with some of these video platforms? We use a suite of Google applications, so that was pretty seamless.

The second, we actually did some work related to COVID. So we found ourselves increasing our workload at that time. I'll just give you two quick examples. One project we work on, we call Clean Sweep. How can we use robotics to be able to disinfect areas that are enclosed? Think about ships as the use case where we weren't able to use ultraviolet light or some disinfectant, and because it's automated with a small robot, how can we do that without exposing other people to COVID? So that was an interesting project, still ongoing. We have a couple of interesting prototypes.

And then the second, how can we provide an early warning signal for someone who might experience COVID and we've employed. You won't be able to see it on the podcast, but I'm wearing a digital watch now and a ring. So two digital wearables, and we're working with a third company that's assessing all of that data, which is data on your temperature, your heart rate. And it's all relative to you as an individual, oxygen in your blood.

And Philips Healthcare, they've developed algorithms that are a predictor of symptoms up to 48 hours before you even know you might be sick. So it is critically important if you think about crews that might be going on a ship, we need to understand whether folks are coming down with something before they get there. And of course, this was a project we had already scoped, but we reoriented it to be specifically focused on COVID. And we've now detected about 350 cases of COVID using these digital wearables.

SAFIAN: This health assessment tool that you've been working on, it sounds like this was something that was planned, but sort of shifted and accelerated in this time. Like in some ways, did the pandemic provide an opportunity for you to move faster through the system that otherwise might've been slowed down more?

BROWN: Yeah Bob, you're exactly right. So we had thought this would probably be a good indicator when someone might be coming down with something. Could have been the flu or something else, but because of the urgency and understanding whether crews might be coming down with COVID – and we saw the negative effects of that on the Teddy Roosevelt – this was able to focus our efforts to look specifically at predicting COVID. And also it helped us enroll many more people in our study. So very important for expanding the trial group, focusing us on one particular disease.

SAFIAN: So you tuned what these devices were measuring to the specific symptoms or things that happen early on in COVID? You held up your watch and your ring. Are all of us going to be wearing these watches and rings? Is the commercialization part of this?

BROWN: Well we often want to work with companies, not just for what they can do for defense, but who have a successful commercial business as well. Those tend to be the best vendors for the military, because that means that the commercial company is going to continue to improve its platform, refine its technology, and then the military is going to be a beneficiary of that.

So it's a huge improvement in terms of the capability that the military gets, if we're working with commercial technology. So you're exactly right. This is a technology that is being pioneered by the military, but Phillips Healthcare, as an example, is very interested in what they can do to make this a commercially-oriented product. So while you might not be able to take advantage of that today, I think you might be able to in the future.

SAFIAN: You were talking about how the funding works. So you oversee only a small part of the DOD budget, right? The vast bulk of the dollars are still spent this old fashioned way. Is part of your goal to develop a proof of concept so that you can demonstrate that that budget should shift? What will it take for this to happen at a larger scale? Or do you not think it needs to happen at a larger scale?

BROWN: Oh my goodness. It definitely needs to happen at a larger scale.

If you think about these game-changing technologies like AI, like cyber, like autonomous systems, these are being developed by the commercial world. So we need a different way of doing business with the commercial world. I would say we need to become a fast follower if we're not the developer of those technologies. How do we understand who the companies are that are developing those technologies, and how do we have a process that makes the Department of Defense as friendly as possible for those vendors?

And we talked about speed and agility being absolutely key in that. We can't work with those companies in the same way we might work with Northrop Grumman or Lockheed. The opportunity costs would be too high and we need them. The leading edge is happening in other spaces.

So the experiment is working, we've delivered 25 different capabilities now to the military that they didn't have before from commercial sources. We've introduced 65 first-time vendors to the Department of Defense. We have started our 100th project. We're doing twice as many projects as we did two years ago. We're seeing 100% increase year over year in terms of the company submissions to DIU. So becoming a little bit more well-known, more companies saying they want to work with the department of defense.

Having said that, your point that you started with, which is we're a very small part of DOD procurement, absolutely true. We're probably affecting in the neighborhood of one to $2 billion of procurement from a startup from five years ago where we were affecting none.

I'm proud of that track record that our DIU team is establishing, but relative to DOD, which has probably bought 1 trillion, 2 trillion, or 3 trillion dollars in that time period, we're a drop in the bucket. So I think that we've proven the benefit of how we work. There's a lot more commercial technology we could be taking advantage of. We need more emphasis on how we scale what DIU is doing to help the Department of Defense.

SAFIAN: I can imagine during 2020 for a lot of smaller businesses, founders and CEOs who are wary about their prospects in the difficult economic climate that doing some work for the government didn't seem like such a bad thing. I can imagine that might have fueled some of this increased deal flow that might be coming your way.

BROWN: Well I think that's right. We're a relatively stable source of revenue if you can get access to it. And the good news for those companies working with us, we've seen recently some fantastic support from Congress. Those congressional oversight committees we talked about earlier have provided their support. And in this year's appropriation, we're in the fiscal year '21 of the government, we received 50% more in congressional appropriations for projects than we had been able to ask for through the president's budget. So we very much appreciate that support and you're right, that helps bring companies along to see the DIU is growing.

SAFIAN: You took on the director job during the Trump administration. Now you're continuing in the Biden administration. What changes in your job as the White House changes?

BROWN: I was lucky enough to pick up an organization that already had a start. And my whole emphasis at DIU has been how do we scale this? So, how do we become much more relevant? And in fact, we have a dedicated team we call defense engagement that is really scanning for what are the most important problems that we can work on. One of the things that Secretary Mattis emphasized to me is we really need to be working on projects that can transform capabilities of the Department of Defense. There's a lot of smaller projects you could do that are interesting, but they don't move the needle on the department's capabilities.

And when he first gave me that charge, I was a bit daunted by how big that that charge was. But when I went away and thought about it, we really do have an impact there. We worked on predictive maintenance for aircraft. That's a technology that the commercial world has used for years. And we went to the vendor of Southwest and Delta Airlines and said, "Could you help us prototype that in the military?" And what you're talking about here is big data, taking the maintenance logs, understanding what is going to probably fail next.

And we were able to show that we can improve the readiness of a particular aircraft by three to 6%. And that may not sound like a big number, but for a lot of these sophisticated aircraft, you're trying to make sure that the readiness level is higher than a 50 or 60% level. So that's how often that plane is not available for a maintenance

problem. So to be able to predict that in advance has huge implications. So that's an example of a technology that we started with the Air Force. We've taken now to the Army and the Marines, applied to ground vehicles, which was predictive maintenance can apply to anything that moves. And now we're talking to the Navy. And maybe the first technology that we've started with and taken across all the services.

So the mission for me at DIU has been how do we scale the organization? The good news is innovation, working with the commercial sector, that's a bipartisan agenda.

We've had tremendous support through the Obama administration, Trump administration, and through the Biden administration. This is something everyone can get on board with, getting access to leading capability for our military and doing it at low cost because it's always cheaper for the taxpayer if we use a commercial solution than if we develop something custom.

[AD BREAK]

SAFIAN: You have a cyber security background as the CEO of Symantec. You mentioned the challenges that the DOD has in security. I know a lot of our listeners in business are much more reliant on remote access and cybersecurity issues in their business also. A greater need, a greater threat. What should folks understand about cyber right now?

BROWN: Well, what folks should understand about cyber is it's a very complex field and almost impossible to defend yourself if a nation state is coming after you as it appears the Russians have done through what's being called SolarWinds, but now as a much bigger attack vector than what we saw with just that one vendor of SolarWinds. So it's difficult to provide the right level of cybersecurity protection for any company out there. But still most of the breaches happen because we don't take care of what I call cyber hygiene, which means we have to continue to ensure that folks are educated not to click on things that are spear phishing, and we've got to make sure that we have the right level of defense. And that means that you're buying the latest products from the commercial markets cybersecurity vendors, and you apply the right patches. So these are basics, and we continue not to be very good as a country, as a society about applying those basics, and therefore we continue to get breached.

Now, separate from that, what this sophisticated attack has shown us is we spend a lot of our energy on building a moat or high wall, a high perimeter, making it difficult to get in the network. We have to move to more of what's called a zero trust philosophy where you have to assume that you've been compromised at least at some point in your evolution as an organization. Which really means you've got to spend some of your resources on hunting, looking for intrusions. So I think there's going to be an explosion in techniques, which I think will help us be more secure.

There's a lot more that we have to do. We continue to not impose enough costs on the attackers, so it makes it easy for them to develop these campaigns. And we have to recognize that when there are nation states involved, we have to figure out what is the right policy that imposes more costs there. The current philosophy of U.S. Cyber Command to defend or hunt forward is a key step in that to try and make sure that we are not in a position of only defending on our own turf, but we're also looking at what adversaries are doing and interrupting some of their operations on their own turf.

SSAFIAN: And the technology that is at the leading edge of being able to provide that protection or that hunting, is that coming from within the government or is that coming from the kinds of partnerships that you're trying to develop?

BROWN: It's both because as companies operate, they don't have the legal authority to be hunting or defending forward as Cyber Command does. That's illegal to take offensive cyber action. And as it should be, we can't have complete anarchy in cyberspace, but the tools to at least understand the intrusions, that's going to come from the private sector.

One of our big DOD partners is U.S. Cyber Command, NSA, and of course the cyber groups within each of our services, Air Force, Army, and Navy each have their own cyber force, and we're helping them integrate the commercial tools with what they might also have developed. They're going to be a lot more effective in their jobs if they can combine the best of what the commercial world has plus what they might know being a government organization.

SAFIAN: For some businesses working with the Department of Defense has engendered protests, sometimes from their own employees, and CEOs can find themselves trying to defend that relationship. How do you address that in the work you're trying to do?

BROWN: Well, I think it's important to understand what the use cases actually are for the Department of Defense. A big mission for our military is humanitarian-assistance disaster recovery. So some of the technologies we're looking for have to do with helping our military carry out that mission. The military is picking a very active role now in COVID response. We know that there's going to be FEMA centers set up to provide additional vaccination, and the medical personnel in the Department of Defense are going to be out vaccinating Americans. So there are a lot of different missions of the Department of Defense. And I think we need to make sure that those professionals have access to the best technology.

So I think part of the answer is understanding what the full complement of things are that DOD is doing. Part of it is understanding that no matter what your beliefs are about the offensive capability of DOD, we need to make sure that those folks have the best information possible, the best tools available to make themselves more productive.

The Department of Defense takes ethics very seriously. In AI, we now have a published set of ethical guidelines. So I think it's a more complex picture than maybe a lot of folks give DOD credit for.

SAFIAN: I want to ask you about China. You were asked by Ash Carter to do a study about China's unique approach to melding technology and security, and it seems you see some competitive risk in the way the Chinese work versus the way things work here.

BROWN: Absolutely. Well, the study you mentioned really brought some attention and light to the fact that not only were the Chinese busy using cyber theft, industrial espionage, but they were also taking the very legitimate legal step of investing in early stage technology. So this highlighted the fact that in 2015, 2016, Chinese investors were involved in 15% of all U.S. venture deals done that year. So China has 500 different investing entities that mirror Western venture capital, growth equity, private equity firms. So they can participate in deals because China's discovered that one of the best ways to bring technology back to China, which is part of their national strategy. One of the best ways to get access to leading edge technology was to follow U.S. venture around, see where they're investing, what companies and technologies they are investing in.

So sure enough, they had a very active program there. So that study resulted in some changes to the Committee on Foreign Investment in the US, an inter-agency group that's responsible for understanding what technology leakage occurs that might be sensitive in national security arenas. And they have some jurisdiction to be able to stop that if they see that that could be detrimental to national security.

But to your broader question, I think we need to recognize that China is very focused on how they transform their economy through technology. It's a very systematic long-term goal, and you can see it in how they're operating. One of the strategies they employ is something called military-civil fusion, and that basically means that any commercial discovery immediately gets transferred to the military. That's their goal. We could argue about how well that's working in China, but that's their goal.

So rather than a DIU, which is trying to provide incentives and work at a faster pace. In China, we know there's no company that is beyond the reach of the Communist Party. If the party reaches in and says, "I want help." If they want access to Huawei's communications infrastructure, the company has no ability as we do in our system to say, “No, I don't think so.” They have to comply.

So it's a very different set of rules for companies in China. They have a national strategy to be stronger in technology. We're talking about satellites, 5G like Huawei, AI through companies like Baidu. And they see that's the key to maintaining the kind of growth they've become accustomed to in the next 20, 30, 40 years. And they're making the investments early on from a science and technology standpoint that they hope will lead to a foundation, again, where they are the leading innovator, where they are setting the

world's standards, and where they don't have to rely on outside countries like the U.S. for some key ingredients to the products they want to make. For example, today, semiconductors, a key ingredient, they have a plan made in China 2025 with the goal of 40% of the semiconductors used in their own electronics, and they're the world's largest electronics manufacturer, to be Chinese-made.

They're nowhere near that goal. They've probably doubled from where they were, probably seven percent to 15%, nowhere near the 40%, and their goal is by 2025 for that 40 to be 70%. So, we don't know whether they'll be successful with their goals, but their goals are clear. They want to displace us. They want all those profit pools to be moving to China. They want to be on the world's stage as the leading technology superpower.

So, we need to think about what is our response to that? And one of our responses needs to be thinking about how much we are investing in science and technology for the future. Part of that role comes from the federal government, because through government investment we can make longer-term, riskier investments that have led to some great innovations in our history, like the internet, like GPS.

Those have come from Department of Defense investments, and think about the tremendous commercial prosperity, the economic prosperity as a country, we have because we've led there, we've set the standards there, it's our companies on the world's stage taking advantage of those technologies. Are we making the investments today that will ensure we have that same position for 20, 30 or 40 years down the road? Our federally-funded R&D has declined precipitously since the ‘60s when we were making big investments during the height of the space program.

SAFIAN: Some Silicon Valley CEOs, as they're facing increased government regulation or the prospect of it, some of them quietly say, "Hey, I'm not monopolistic because some of my biggest competition is coming out of China, and if you tie my hands, the Chinese government’s on the other side is just going to keep going, and we're going to lose in the long run." Do you feel that way? Do you see any of that argument?

BROWN: Well, I think there is an argument there for ensuring that our antitrust philosophy recognizes that these are competitors on a world stage, but I also think there's an argument for ensuring that we're encouraging innovation. And if our philosophy is limited to we only want large, national champions the way China thinks about the companies they want to put on the world's stage, we're probably not doing the best from an innovation standpoint. So, we need to think about the response to China as what brings the best of what the U.S. can offer.

In some cases, that may not be applying antitrust laws if we look at competition on a global scale versus U.S. In other cases, I think it's making sure what policies we have to make sure we’re stimulating increased innovation in the economy. And part of that stems back to what we talked about before, are we making the investments as a federal

government that provide the breakthroughs that will lead to future innovative companies coming on the scene.

SAFIAN: What's at stake in this moment for DIU?

BROWN: I think that it's a critical inflection point as we think about the Department of Defense facing increasing budget pressure, because there's other pressures we have for our spending dollars as a government, to be increasingly efficient. And efficiency, part of that means we've got to be drawing on all the innovation that's happening across the American economy and working with more commercial technology.

So, DIU today is just scratching the surface on what could be done, both in getting more leading edge technology to the military, and making sure that's very efficient from a taxpayer point of view, because it's always going to be less expensive to leverage commercial technology and the tremendous investments that are being made by venture capitalists, private equity, and other actors across the economy than to do something custom. So, we need to make sure that DIU is very effective in its role and has the possibility to expand, to provide even more value and impact to DOD.

SAFIAN: You don't have a specific military background, so as you come into this job, do you miss being in the commercial sector? What about the military is satisfying or frustrating?

BROWN: Well, you're right. I have no military background, which makes me a bit unique in the Department of Defense and at DIU. But what has been compelling – and if anything, it's been the best job I've ever had; I'm just enjoying it so much – is the mission. There couldn't be a more important mission, as we've talked about. It's critical that we get leading edge capability to our war fighters. And I'm working with an incredibly talented set of folks. And then the folks that we get to work with at the Pentagon and the Congress, it's a really interesting mission working with some great people who are also aligned.

I think that one of the benefits of having a commercial background is to be that bridge. I understand the pressures that young companies are under, and those CEOs, and so we can help bring that message to the military in terms of: How do we need to change how we do business and be that fast follower so that we can be the right type of customer for those companies that we need to work with? So I think that the translation is something that's important to bring to the job.

SAFIAN: But you're having fun.

BROWN: I am having fun. I have never worked on something that is so mission-oriented with a more talented set of folks, and that's inspiring. It's very motivating to work with the people I'm able to work with on such meaningful work.

SAFIAN: Well, Mike, I really appreciate you taking the time to share all this with us, and thanks so much for joining us.

BROWN: Oh, thanks for having me. I really enjoyed the conversation, Bob.