Transcript of Episode 16, “Concealing and Revealing Clandestine Military Capabilities”

Originally released on June 22, 2021

[Note: This is a rough transcript of the audio recording, based on digital transcription and human review.]

[00:00:00] One, two, three go.

Morgan Kaplan: [00:00:18] Hello, and welcome to *International Security* “Off the Page.” On today's episode, we are talking about when and why states reveal their clandestine military capabilities. We'll also discuss the role of the private sector in industry and helping develop these capabilities as well as concealing them.

I'm Morgan Kaplan, the Executive Editor of *International Security*. And we'll be speaking with Austin Long, the author of a recent *IS* article with Brendan Greene titled “Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition.” And a little later, we'll go off the page with E.J. Herold, who is the Executive Director of the International Institute for Strategic Studies-Americas and was [00:01:00] previously the NATO Deputy Assistant Secretary General for Defense Investment.

Benn Craig: [00:01:09] Belfercenter.org/offthepage is where you can find past episodes as well as supplemental reading materials. It is also where you can subscribe to “Off the Page” on your favorite podcast platform.

Morgan Kaplan: [00:01:17] Austin Long is Vice Deputy Director for Strategic Stability in the Joint Staff J5 at the Department of Defense. The views expressed here are his own and do not represent the views or policy of the Joint Staff, the Department of Defense or any other entity. Joining us now we have Austin Long, who's written a fascinating article for us with Brendan Greene called, “Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition.”

Austin, welcome to the show.

Austin Long: [00:01:51] Thank you very much for having me. It's a pleasure to be here.

Morgan Kaplan: [00:01:54] So what is the, the question that you guys are trying to answer in this manuscript? And what's the main argument?

Austin Long: [00:01:59] We tried to do a couple of things in the manuscript in terms of laying out the problem. First, is sort of defining a clandestine capability.

So all military capabilities benefit from some degree of secrecy, right? If the adversary doesn't know an attack is coming, obviously the attack is more likely to succeed in many cases. This is a little different than just sort of normal secrecy or normal surprise in that, because the capability depends on a, an adversary vulnerability, its military utility may not

just diminish, but may go to zero if the adversary becomes aware of the vulnerability and fixes it.

So if you think about something in the cyber realm where there's an exploit, where there's a problem in your software, that somebody can take advantage of, if, you know, you have that problem; of course, you know, most of your listeners in their daily life will have gotten a security update on one piece of software or another; it can be pretty easy to fix at least in theory. So it's very difficult to talk to an adversary to reveal this capability to an adversary without putting it at risk, right?

So I have a very powerful capability. I tell you [00:03:00] about it to deter you or to shape our competition. You fix it, the capability goes away. So the question we really grapple with is if you accept that these capabilities exist, capabilities with these characteristics, do they inevitably create the kind of private information that dooms deterrence to failure, right?

Because I can't tell you what my real capabilities are, you can't maybe tell me what your real capabilities are. We both sort of are more optimistic about war outcomes and therefore deterrence is more likely to fail. Or, are there ways to reveal capabilities potentially that don't put them at risk?

And if so, how would you know what capabilities you might be willing to risk and under what conditions? So the answer we come up with is yes, there probably are ways to signal these capabilities. Some will be entirely too sensitive to put at risk by talking to the adversary about them or revealing them.

Others will be of a nature where you're more willing, willing to put them at risk. And so being good social scientists, the answer must lie in a, in a two-by-two matrix. And the two [00:04:00] variables we sort of would key in on, which we don't think is sort of an exhaustive list, but we think is a good start for thinking about the capabilities.

One is how unique the capability is in your sort of portfolio of capabilities. So if this is your one way to do something, it provides unique warning, it provides unique ability to hold adversary capabilities or values at risk, that means you're going to be less likely to put it at risk. Whereas if it's just one among many capabilities, it's not as unique. You'll be more likely to put it at risk because if you do lose it, if the adversary does figure out the vulnerability and fixes it well, you've lost the capability, but it's only one a month. So that's sort of one axis of variation.

The other is how easy is it for the adversary to fix the vulnerability in question? So in the cyber realm, the vulnerability fix may be quite easy and not take very long, just fixing a few lines of code, distributing a patch, et cetera. Others that require more extensive changes in physical world, the adversary may be able to fix the vulnerability, but it will take them such a long time that you're more willing to put it at risk.

So from a [00:05:00] revelation perspective, the ideal capability is one that's not very unique, but the fix of the vulnerability for the adversary takes a long time. You can reveal that all day long, because if you lose it, I don't care, I've got other capabilities, but even if the adversary finds out what the vulnerability is, it's going to take them a long time to fix.

Obviously the other end of the spectrum is it's a unique capability that the adversary can easily fix the vulnerability. Those will be the deepest, darkest secret forever, right? Unique, very fragile, et cetera. The other two quadrants of the two by two are a little more mixed in terms of estimating how long it would take an adversary to fix a vulnerability for a unique capability, et cetera. So that's sort of the, the argument that is a nutshell is sort of structuring thinking about these capabilities, and as I say, I don't think this is an exhaustive list of variables that go into thinking about clandestine capabilities, but we think it's a good initial framework.

Morgan Kaplan: [00:05:46] You make this interesting argument that the kind of utility of revealing clandestine capabilities is unique to a peacetime environment as opposed to a wartime environment. Can you tell us a little bit more about why that's the case?

Austin Long: [00:06:00] Sure. So we actually look at sort of three conditions where you might want to reveal these capabilities.

The first is war time, and we think, you know, the drivers of war time, particularly if it's a high intensity conflict with maybe existential stakes, you're just going to use the capability. You need to win the war and that's how you're going to affect political outcome. So there's not really much question about whether you're going to put the capability at risk. You're going to break the glass, take the capability out and use it to win the war and shape political outcomes that way.

The second is a crisis scenario where maybe war is not definitely coming, but looks likely. And so maybe you reveal a capability or a set of capabilities in crisis to deter escalation into war. And we think that that's obviously something you can do, but we think the utility is limited unless you can lock the political gain, right? So if you reveal these capabilities to an adversary and the adversary terminates the crisis, but you haven't locked in the political gains, let's say a territorial dispute, they can go fix all the vulnerabilities that you showed them they have, and then come back and readdress the problem in two years.

So you've expended all these capabilities in a [00:07:00] sense, and only bought yourself a couple of years. And that may be worthwhile in some circumstances, but we think overall that's not particularly useful.

And the third scenario is peace time competition, right? Where you're in a competitive environment. You're trying to shape how your adversary acts to get political gains, also to shape maybe their force structure in ways you find to be advantageous. We think that's where the real utility of capability revelation is, shaping that long-term competition, precisely because you can lock in political gains in that competition.

Morgan Kaplan: [00:07:27] And so how does this challenge, the conventional wisdom on what's out there about when states will conceal or reveal their clandestine capabilities?

Austin Long: [00:07:34] The default, at least in the academic literature, is that capabilities will either always be concealed or will be broadly understood and therefore not clandestine, right?

So states will always keep their war plans secret from their adversaries to the extent that they can. And that, that just becomes private information. And we, we argue that in fact, some of these capabilities, there's utility in revealing in order to shape or deter competition. So we're, we're [00:08:00] challenging the conventional wisdom that the default setting is always and shall ever be to conceal.

And in fact, both scholars and policy makers should recognize that there's utility in revelation, at least in some circumstances.

Morgan Kaplan: [00:08:11] And you've done some fascinating case study work on these issues, particularly with anti-submarine warfare. Can you tell us a little bit about how this argument operates in practice within that case?

Austin Long: [00:08:22] Sure. So the cold war anti-submarine warfare case is particularly useful because you get some variation over time. And, it was also a pretty important capability. I'm not going to talk too much into the technical details, but for those of your listeners who have not seen the movie *The Hunt for Red October*, I certainly recommend it.

So, anti-submarine warfare is essentially finding adversary submarines. In the case of where we're looking at, it's focused on US ability to find and hold at risk Soviet ballistic missile submarines. And there are a couple of different time periods in the initial time period in the 1960s.

This is a unique capability for the United States. The United States believes it provides very good [00:09:00] warning of Soviet intentions for major war. There's not a lot of other ways to get that kind of a warning, so it's a unique capability. United States also believes as the United States is improving its capabilities in the submarine realm, the Soviets are not going to be far behind. So this is a vulnerability.

If the Soviets understand they'll be able to fix pretty easily and they may fix it over time anyway. So this is a very tightly protected capability for the United States. Unfortunately, and here's where exogenous things come into play, the US capability was revealed. Not intentionally, but by a Soviet intelligence success spy by John Walker and his compatriots in the Navy that revealed this capability to the Soviets. But, I might add, not to the general public.

So the United States took a while to figure out exactly what had happened. The Soviets radically changed their submarine program. Rather than deploying ballistic missile submarines close to the United States, they built much longer range missiles and began deploying them much closer to the Soviet Union, where they could protect those submarines from US anti-submarine forces.

So the US had [00:10:00] to do quite a lot to try and regain some of the capability – find and hold at risk Soviet ballistic missile submarine – but it succeeded. The difference is in the second period, which is roughly starting in the 1980s, the US was much more public and revealing that it had regained some of these capabilities because it had become much more confident that the Soviets had vulnerabilities in how they built submarines that they would have real trouble fixing, even if we revealed a lot about the capability.

It was just very difficult for a variety of reasons for the Soviets to build truly quiet submarines, that would make them much harder to find. So the US, particularly Chiefs of Naval Operations, but others were much more public and things like congressional testimony about those capabilities.

And it was for the clear reason of shaping the military competition with the Soviet Union. And in one of our interviews a former US policy maker referred to it as, we wanted to show the Soviets the mountain, that is the mountain of US military industrial capability, and that the mountain was too high to climb in terms of shaping that late Cold War competition.

So from that perspective, I think the revelation in the late Cold War [00:11:00] of US anti-submarine capabilities was actually fairly effective.

Morgan Kaplan: [00:11:04] So what's the big policy takeaway of today's environment?

Austin Long: [00:11:05] There is often, though not always, an instinct to conceal capabilities for advantage. So I think the policy implication is, even though it may put capabilities at risk, a judicious and well-thought through revelation of capabilities can actually bolster deterrence and more important, it can shape the nature of the competition.

If you want to shape that competition, policymakers have to have a thoughtful strategy for how they reveal clandestine capability. So I think it's vitally important in the 21st century.

As I said, I think these capabilities, you know, by their nature, they're very difficult to sort of count. But I think given where technology is, the emergence of things like threats in the cyber realm, threats to physical supply chains, threats in space, I think there's just a host of multiplying opportunities for clandestine capabilities for all great powers and even, you know, not great powers to cultivate.

So it's a, I think an important topic and one that's only going to grow in [00:12:00] importance in the coming year.

Morgan Kaplan: [00:12:01] Fantastic. Well, Austin, I only have one more question for you and that is, are you ready?

Austin Long: [00:12:07] Ready for what?

Morgan Kaplan: [00:12:08] To go off the page?

Benn Craig: [00:12:14] If you enjoy listening to Off the Page, you'll enjoy reading our quarterly journal *International Security*, which is edited and sponsored by the Belfer Center at Harvard Kennedy School and published by the MIT Press. To learn more about the journal, please check out Belfercenter.org/is.

Morgan Kaplan: [00:12:29] E.J. Herold is the Executive Director of the International Institute for Strategic Studies-Americas. He was previously the NATO Deputy Assistant Secretary General for Defense Investment, a Business Development Executive at IBM, and he is a retired Colonel in the US Army. E.J., welcome to the show.

E.J. Herold: [00:12:49] Oh, thank you very much, Morgan. It's a pleasure to join you.

Morgan Kaplan: [00:12:51] Well, so we thought we'd start first by asking what your general thoughts were on this manuscript by Brendan Greene and Austin Long on to [00:13:00] conceal or reveal?

E.J. Herold: [00:13:01] Well, I thought it was an interesting premise. The notion that the peace time considerations on clandestine operations differ from war time considerations and offer the opportunity to signal and to do things diplomatically that you might not otherwise be considering, caught my attention.

Morgan Kaplan: [00:13:19] One question we had is, as someone who's had a tremendous amount of experience in the intersection of defense industrial collaboration, you served for six and a half years as Deputy Assistant Secretary General for Defense Investment at NATO, as well as at IBM in Brussels, do these conversations about when to conceal or reveal military capabilities come up in these conversations across the sectors?

E.J. Herold: [00:13:41] I wouldn't say that they come up explicitly as an acquisition question, but they are implicit in the discussion of acquisition initiatives, where the government is setting or the international organization is setting its priorities and asking for a response from [00:14:00] industry for what their capabilities are.

And it comes up for the industry folks in their informal discussions as they're sensing with their client base, what the client is looking for versus what they have to offer. I think the real issue here when you have this discussion around the article is, technologically as technology advances, what do we want to protect? And, what do we have to protect versus what can we use for political and diplomatic purposes to advance the interests of the state?

Morgan Kaplan: [00:14:35] And to what extent is there kind of disagreement or friction between the two over what is appropriate and not appropriate for sharing technology? And I asked that because you've sat on both sides. On the one hand you've been in a position at NATO. And on the other hand at IBM, you were at a position representing the company with NATO.

E.J. Herold: [00:14:52] Oh, I would say there's absolutely a tension, mostly because from the industry side, there's a profit motive. And, [00:15:00] so whatever serves the interests of the corporation to advance sales is something that they want to pursue.

But that said, and the interesting thing that I found, because there was a sort of suspicion of industry from non-industry folks, whether it be at NATO or when I served in uniform, I find that the industry partners are actually just as concerned about maintaining national or international organization security and advantage as those that serve in uniform or those that are on the government side, because there is an imperative not to do harm.

So while the profit motive is strong, the maintenance of relations with the client base are actually stronger. And so while there are certainly anecdotal evidence to the contrary where individuals have done things that were not in a nation's interest or in an international organization's interests because they were favoring the profit [00:16:00] motive, I would say

that by and large, the industry that is pursuing business with governments and with international organizations is highly sensitive to maintaining secrecy and advantage for their clients and not doing anything that will jeopardize future sales or future business with that client.

Austin Long: [00:16:18] There's variation in that across firms. Not that any firm doesn't take security seriously, but I'm just thinking you have sort of traditional defense contractors that are very used to dealing with very sensitive materials. But increasingly, and we certainly see this in the space and cyber worlds. A lot of the firms that are starting to do business with defense entities, you know, they may have more of a commercial presence in data technology in software or in sort of space startup stuff.

So I wonder if you see any variation between the sort of big defense pine type firms and maybe smaller startups that aren't quite as accustomed to that world?

E.J. Herold: [00:16:55] I think if there is a difference, it comes from a number of motivations. [00:17:00] In the first instance, the tech world that you cite is not predisposed to secrecy.

It's about sharing open standards, about creating the internet of things and making sure that those things that are operating in that domain are operating in a way that can talk to each other, communicate with each other and create that network advantage. It comes from the products they're developing.

But when confronted with the imperatives of the defense sector, I think that there is an understanding that develops quite rapidly with those companies about what is necessary, what is proper and what are the constraints that the government clients impose for sovereignty and national security and in any profit making organization, their interest is in pleasing the client.

Where I do see some differentiation is, and there are the famous examples that we're seeing out of Silicon valley, where companies have put [00:18:00] their foot down and said they don't want to deal with the government because they don't want to provide advantages or capabilities to purposes that they disagree with.

That's an education process, and that's a burden on both the company leadership and the government side to communicate in ways that we assured the employees about the needs for their products in the national security space, as well as why secrecy or confidentiality is a requirement or a need vis-a-vis potential competitors.

Morgan Kaplan: [00:18:35] So far we've been talking about this almost as if there's kind of like a binary relationship, two actors, right? There's the governments, the militaries involved, and then there's a company from the private sector, but this obviously gets complicated very quickly once we factor in that some military technologies, right, are joint products of multiple nations. And some technologies themselves are built by [00:19:00] multinational corporations that have different components all across the world.

And so, I guess the question to both of you is, to what extent does this create issues in both companies' understandings of their responsibilities to maintain clandestine technology, but

also how countries themselves, when they're developing it, did they have some sort of friction or disagreement over what the ultimate, I guess, kind of public nature of that technology will be?

Austin Long: [00:19:27] I think it actually is quite challenging and it affects, you know, at least in the multinational military operation sense, it affects everything from acquisition to planning and operation. So if you have a system that has very sensitive capabilities, you don't want adversaries to know about, and it's in a multinational context, how do you decide what allies are able to see and plan, what capabilities?

If all allies don't have equal access to sort of understanding the capability, then how do you plan? Do you just have, you know, some subset of [00:20:00] allies that have full access and they do the planning and then hand off completed plans to operators from other nations. I mean, you can do that, it gets very challenging.

I would just say from my own experience, this is not purely a sort of super advanced technology issue. A lot of it just comes down to the, to the sharing relationship. And so you can just compare the sharing relationship between the Five Eyes nations. That is to say the US, UK, Canada, Australia, and New Zealand, which have a very special communications-intelligence relationship with a lot of other countries, because those relationships are not as closed to sharing, it's not as transparent, it can become challenging to plan when you have five eyes nations in a coalition, along with other nations.

So I think it's a, it's a real challenge. I've seen it mostly on the multinational military side, but I'm sure the firm side is also challenging.

E.J. Herold: [00:20:49] Yeah, I would agree with you Austin.

And you know, one of the things that was really a watershed moment in this whole discussion was the decisions taken by General McChrystal in [00:21:00] Afghanistan, where the security of information was based on a need to know, and they turned that argument around that to a need to share. And the classic example was protecting sources and methods that determined that there was a, an IED on a route that was going to be used by ally X.

Do you tell that ally, when you know that their patrol is headed down that route or do you not tell them because you don't want to compromise sources and methods? These became untenable questions. And so the argument that was made by General McChrystal was we have to turn this discussion around. We have to decide what do we need to share? And we have to determine how to protect sources and methods and still be able to protect our allies and partners so that the success of the mission comes before this question of security and information sharing. And I think that's applicable in the relationship between industry and governments as [00:22:00] well.

And the discussion becomes one of the information that we have needs to be protected because it gives us an advantage while you may, industry, want to profit from it, your profit will come from your sales to us as a government entity. And eventually as the technology matures or a capability declines in effectiveness over time, because potential adversaries

can counter it, then you can sell to others because it's less sensitive. And your opportunity is in the long-term relationship with the government rather than a short-term transactional relationship.

Morgan Kaplan: [00:22:36] So far, we've been talking about kind of conscious choices, right? By which governments, militaries, private sector actors will agree to certain terms of concealing or revealing technology.

But it seems like a lot of what gets out there happens through nefarious channels, right? Whether it's hacking or leaks of some nature. And this kind of brings up the conversation of to what extent [00:23:00] companies and militaries feel competent today that they actually have control over their ability to conceal or reveal technologies when it's useful to them?

You know, the cases, Austin, from, from your manuscript, are Cold War cases, where I could be completely wrong, but it seems like it would be easier for states to conceal secrets, given the absence of the internet and other things. Is this an issue that is kind of falling out of the hands of governments and the private sector more as technology advances and it becomes easier to kind of hack into places and take secrets 0r is this still a decision that's in the hands of governments and companies to the same extent as it used to be?

Austin Long: [00:23:38] So I would say it's always been a challenge and Brendan and I grappled with how you include that factor of your ability to protect secrets, if you choose to protect them.

And then the converse is the adversary's ability to, to penetrate your defenses. And it was just something we could never come to a satisfactory answer on how to, how to capture it. It's a real issue. So in the case, we look at it, the Cold War [00:24:00] anti-submarine warfare, you know, the, the central revelation was not by choice.

It was because of the Walker spy ring sort of revealing to the Soviets exactly how vulnerable they were in the submarine warfare department, you know, subsequently the US made decisions about revelation deliberately, but that initial revelation, as you say, was absolutely out of their hands. So I don't know if it's getting worse now.

It's always been a challenge, but it certainly continues to be a challenge. And I think it varies over time. You can read a lot of the press reporting about data exfiltration from the US defense industrial base. That was clearly a failure to protect secrets. Now, how sensitive any given secret was exfiltrated was, it's difficult to say, but there've been a variety of steps taken to try and shore up those defenses. But whether that's been successful or not, is not readily apparent.

E.J. Herold: [00:24:48] Well, I would agree that the problem seems to have gotten worse. And the example that most readily comes to mind is the Chinese, I think it's the J-20, which is the replica or the lookalike to the F-35 [00:25:00] and famously months of access to Lockheed Martin's proprietary information now gave the Chinese the opportunity to exfiltrate some of the technological capacity of that fighter.

And the internet has laid bare the risks of information theft and unintended information transfer. Now, fortunately there is a good deal of effort being put into securing internet access and securing information. But I think that we will continue to be fighting a difficult battle in cyberspace with information theft, disinformation, and the ability on both sides to try to diminish the importance of information stolen as a way of deterring or keeping those that may have stolen something from understanding its true value and intentional use. So it's a very complex environment and that's one of the things that I saw [00:26:00] in the IT industry. They still, in all of their vaunted capacity, don't have good answers for preventing this type of activity on the part of bad actors.

Morgan Kaplan: [00:26:11] You know, E.J. brings up an interesting point that we've thought about often, which is who's responsible for the security of information and cybersecurity, right? One of the big tensions within the national security-cyber security sphere is, is the government responsible for securing the cyberspace of private sector companies? And I wonder to what extent that this disagreement, or kind of a misalignment of who believes it's their jurisdiction to protect information may actually lead to more cracks and more opportunities for others to thread the needle between where there's no overlapping systems. But it's a question I think that's going to be one of the key ones for cyber security going forward.

E.J. Herold: [00:26:50] Well, I would agree with you, but you know, this is the tension of living in a free and democratic society. And the notion that the government has [00:27:00] the responsibility for securing cyberspace kind of flies in the face of liberal free market democracy and the notion that industries should protect themselves, government should protect government systems.

And part of the challenge in cyberspace is that we've advanced so rapidly into this new unknown that an awful lot of people are learning in an ad hoc fashion, how to operate in cyberspace and as a result, so-called cyber hygiene or the training necessary for individuals to secure themselves and to secure their actions in the internet and in cyberspace don't happen in a uniform training system.

As a result, you get inadvertent leaks, inadvertent compromises, or simply uneducated lapses that result in vulnerabilities that are exploited by competitors and potential adversaries.

Austin Long: [00:27:57] I would just say though, that there's always a [00:28:00] certain amount of opportunity in these things.

So the ability of adversaries to access your systems, if you're, if you're cognizant of it, it becomes a means to potentially provide some insight into a capability while protecting maybe the sensitive nature of the capability. So I think the J-20 example is interesting. It's not clear, you know, as you alluded to, how much the sensitive materials technology was accessed versus just the, sort of the basic shape, which is important, but maybe not as important.

And I think there are potential opportunities to provide disinformation through some of the channels, if you so choose. So it becomes, it becomes a very complicated thing when you're able to take lots of data. You're not always sure that the data's right, maybe some of it is contradictory and maybe some of it is intentionally misleading.

Morgan Kaplan: [00:28:44] One area I want to push the conversation and apologies if this gets a little too meta, but one of the key points of Greene and Long's article is that the utility of revealing clandestine capabilities is unique to a peacetime [00:29:00] environment and not a war time environment. But to what extent today are we able to kind of distinguish between those two types of worlds, right?

Are these two worlds becoming any more blurred today, peacetime and wartime, than they were at the time these cases were looked at? And again, that ties directly back to this idea of cyber conflict, hybrid conflict, low level conflict between states. Do you believe there is more gray area between war and peace time environments today? And if so, does that affect the way that the argument applies?

E.J. Herold: [00:29:31] You know, the one thing that I found fascinating about the article was the example of anti-submarine warfare and, you know, in the popular culture, most of us have seen *The Hunt for Red October* and appreciate the complexity of that undersea environment and the advantages relative disadvantages that we played with the Soviet Navy over time.

I don't think it applies as a direct comparison to the cyber realm today, or [00:30:00] rather, I would say that that was an environment that was very closely bound by physics and the capabilities that were developed by industry to address that environment. Cyber has opened up a, a seemingly unbounded opportunity for nefarious actors with very little investment to be able to harm societies, governments, and industry.

And the example that I go to is what happened with Crimea and Ukraine with little green men and hybrid warfare activities on the part of the Russians. We simply got surprised and that there was a lack of an ability to adequately address what we were seeing until the situation was beyond the capacity of governments to adequately influence.

So the cyber realm has opened up a different calculus. And the question of advantage from the handling of information and [00:31:00] whether or not to reveal or not reveal, I think governments and if we just look at US governments are struggling with what that looks like. You know, you've had release of seemingly classified information by every administration in recent memory for different purposes.

And I think particularly in the case of the US government, people are struggling with, when it makes sense to reveal things that previously might have otherwise been maintained in secret. And we don't know the answer to the question that is posed by the work of Greene and Long.

Austin Long: [00:31:34] I think that's right. And I think even within the cyberspace, it varies from capability to capability.

So the ability to cross into air gap networks is a significant hurdle. It's clearly not an insurmountable one, but it would make those capabilities potentially more unique, which I think is one of the key variables we, we talk about. And also potentially easier for the adversary to fix. And I [00:32:00] think that what you highlight there is one of the big differences with the cyber and the physical realms is it's not always easy to fix cyber vulnerabilities, but if you become aware of them, and as you say, you're disciplined in your personnel side, but cyber hygiene and, you know, making sure patches are applied and things like that, the fix for the vulnerability can be fairly rapid and potentially not that costly.

Whereas as you say, in the physical world, when you're bending metal, when the Walker's firing revealed to the Soviets, how vulnerable they were in the undersea domain, they had to reattack their entire ballistic missile submarine design, and came up with some weird sort of interim solutions before they shifted to a bastion strategy. So that was hugely expensive and took a lot of time.

Morgan Kaplan: [00:32:41] Great, well E.J., we have a tradition here on the show, which is before we close out an episode, we like to ask our special policy guest what advice you'd give junior scholars, practitioners, service members based on your years of experience.

E.J. Herold: [00:32:54] And so this is a great question. And it's one that I've actually spent a fair amount of [00:33:00] time, not just thinking about, but doing something about. In many jobs that I've had, I've had an opportunity to influence younger folks following in my footsteps, whether it be in uniform, in business or international diplomacy, and because I've had so many different roles and you alluded to the fact that I'm a bit of a unicorn in the sense that I've served in uniform, industry and international diplomacy, and now I'm back in the think tank world.

I've done all of these different things sometimes by choice and other times, because circumstances pushed me into jobs that I didn't necessarily want, didn't necessarily appreciate at the time, and didn't necessarily think that I would be very good at. But what I've found over time is that when you are put into an unfamiliar environment or to an unpleasant environment, something that doesn't fit your self-image, your planned career path, if you embrace where you are and learn the requirements of that job, if you [00:34:00] embody or embrace the tasks and the learning required to be good at what you're doing, you have now given yourself an unparalleled gift.

You have a new tool that goes into your toolbox and you don't know where that tool is going to be required and when you're going to need it again, but it's there. And someday in the future, you end up in a job that prior explicit training in, and yet those tools that you've developed over time become valuable and enable you to succeed rapidly.

And I'll give you a good example. I was required in military service to, because I had been injured and couldn't perform my primary duties, I was put into a job that was not coded for somebody at my skill level and seniority, and yet it needed to be done. So I did the job and I was a battalion motor officer, and this was something that I didn't aspire to, didn't particularly want, but it was important to the readiness and preparedness of a unit for deployment.

So I learned [00:35:00] it. I did it. And then later, in my job at NATO, in my first week on the job, I was called upon to answer questions about equipment preparedness and suitability within a NATO context, that I was able to use the skills that I had developed way back as a first Lieutenant in uniform, some 30 odd years prior.

So my point to young people is never turn up your nose at a job you're asked to do, or an opportunity that you're given, learn from it, take that skill. Put that tool in your toolbox, and someday, in some way, it will come in handy in the future and you'll be better off for it.

Morgan Kaplan: [00:35:38] That's really fantastic advice. E.J., Austin, I want to thank you both so much for providing a fascinating conversation and for joining us on the podcast today.

E.J. Herold: [00:35:47] It's been a pleasure, thank you very much.

Austin Long: [00:35:48] My pleasure as well. Thanks very much.

Julie Balise: [00:35:58] Off the Page is a [00:36:00] production of *International Security*, a quarterly journal edited and sponsored by the Belfer Center at Harvard Kennedy School and published by the MIT Press. Our program is produced and edited by Morgan Kaplan, the Executive Editor of *International Security*, the Associate Producer and Technical Director is Benn Craig, digital communications by me, Julie Balise, production support by Carly Demetre.

Thanks to our intern Elizabeth V. Silva for additional assistance and a special thanks to Hilan Kaplan for composing our theme music.

Upcoming episodes, and additional material for Off the Page can be found online at belfercenter.org/offthepage. All articles from the journal can be read at belfercenter.org/is.