Cyber Strategies and Successes: A Conversation with National Cyber Director Harry Coker, Jr

January 7, 2025

Featuring Harry Coker, Jr. and RADM (Ret.) Mark Montgomery

MONTGOMERY: Good morning. Welcome, and thank you for joining for today's event. It's hosted here by the Foundation for Defense of Democracies. I'm Mark Montgomery. I'm the senior director of the Center on Cyber and Technology Innovation here.

First, I want to say, Harry, I think we know who all our true friends are as we look out.

(LAUGHTER)

OK, it's Tuesday, January 7th, and today's fireside chat is going to cover the successes, the experiences, the lessons learned in the future of the Office of the National Cyber Director throughout and beyond this inaugural term. We're pleased to have you here for this conversation, some in person, more than I expected, some tuning in live, some listening to the podcast.

Four years ago, Congress created the Office of the National Cyber Director to serve as the president's senior advisor on cybersecurity, implementing national cybersecurity strategy, supporting whole-of-nation cyber resilience and working with OMB, the Office of Management and Budget, to align federal resources to combat the growing cyber threats from criminals and nation-state actors.

The NCD provision in the NDAA actually came from the Cyberspace Solarium Commission, where I was executive director and observed the commissioners come to this conclusion. The commissioners recognized that a cyber resilient nation required strong leadership at the White House, and thus, they argued for the creation of the ONCD. Since then, the ONCD has led the charge to develop a new cybersecurity strategy and executed dozens of technical, governance, workforce, and policy solutions that I know Harry'll talk to.

So joining me today is the national cyber director, Harry Coker, Jr., my friend. Today, Director Coker is going to provide some prepared remarks, then he and I will sit over there and discuss answers to the questions on how the office has aided in thwarting and deterring U.S. adversaries in cyberspace.

When President Biden nominated Director Coker, I noted that he was a leader with superb qualifications and a distinguished record in government. He's done an exceptional job of fulfilling the role. It's always good to be proven right. Thank you.

(LAUGHTER)

I've had the pleasure of talking regularly with Dr. Coker and have seen firsthand how thoughtfully he approaches finding solutions to hard cyber problems.

Before I turn it over to Director Coker for his opening remarks, a few words about FDD. For more than 20 years, FDD has operated as an independent, nonpartisan research institute exclusively focused on national security and foreign policy. As a point of pride and principle, we do not accept foreign government funding. For more on our work, you can visit our website at fdd.org, follow us on X or on Instagram or subscribe to our YouTube channel. We're basically everywhere.

You've heard enough from me, so let's get to why you're here today, and I do, again, appreciate the one who came here. Please join me in welcoming National Cyber Director Harry Coker, Jr.

(APPLAUSE)

COKER: Thank you, Mark, for the introduction and for your leadership and partnership in making our country more cybersecure. And I don't want to forget about your 32 years of service in the United States Navy, where you made our country even more secure. So thank you, shipmate.

Thanks to the Foundation for Defense of Democracies not just for hosting this event, but for the counsel that you all have provided for decades. And thanks to you all, this distinguished audience in the room and online for your contributions to the field. It's – as Mark said, it's delightful to see our good friends at – here, and we appreciate that, and Happy New Year to you all.

But also, Happy New Year to the Office of the National Cyber Director and happy birthday to the Office of National Cyber Director. We turned four just last week. And to the members of that ONCD team that are present and those that are past, I sincerely thank you. So I'm just so proud of what we have accomplished together. Today, I do get to talk about this young office, what we have created, and thanks to your dedication, your thoughtfulness and perseverance, again, I sincerely and humbly thank you.

And let me say at that – at the outset that the Office of the National Cyber Director stands on the shoulders of patriots, the cyber leaders from the Clinton, Bush, Obama and first Trump administrations. They worked to bring stakeholders together, increase information sharing across all levels of government and the private sector and build out cyber capabilities both defensive and offensive. Those on the Cyberspace Solarium Commission and our partners in Congress who identified gaps in federal coordination and laid out how to organize and pursue a whole-of-nation approach to cybersecurity. We are here today thanks to their wisdom, vision and ongoing support.

And I personally am proud to continue the work of the inaugural National Cyber Director, the Honorable Chris Inglis, who famously started the Office of the National Cyber Director as an army of one, or as he might say, an Air Force of one.

(LAUGHTER)

His tremendous foresight continues to serve us and this nation well.

Also to Kemba Walden for coordinating, staffing, drafting and implementing the National Cybersecurity Strategy, and the other former national cyber director, my dear friend and colleague, Drenan Dudley, who provided vital guidance to interagency partners, helping them think through the budgets they needed to deliver on their cyber missions.

Now, after decades of rapid growth, it is worth taking a moment to consider how important the cyber world has become to virtually every American, especially with all the digital advances that we have and – to live and to work just since the pandemic. Now, we've been saying it for quite a while, but now, it is clearly and obviously true: The online world – excuse me – the online world is an absolute necessity for daily life, just as fire has been throughout human history. Fire provides warmth, power, and light, which have enabled the rise of civilization. But uncontrolled fires have caused terrible harm.

Likewise, the march of digital innovation, for all the good it has done, has created vulnerabilities and harms of its own. When we consider how to tame fire, it's tempting to focus only on building the great – the greatest team of firefighters, brave people ready to react to the latest conflagration.

But that's not enough. We also need to prevent fires. That requires building codes, rules for how buildings are designed and constructed so that they can protect their occupants, and they're resilient when fires do flare up. Prevention also requires implementation. Building codes are only valuable when they are adhered to.

So we set out to proactively establish and implement tough cyber building codes. But first, there were some fires to fight.

As this team came into office, the SolarWinds hack had given Russia broad access to a swath of American organizations, including federal systems. President Biden declared that the federal government needed to lead by example, and he issued Executive Order 14028. And as a result, we have been moving our systems towards more resilient, zero trust architectures, taken more steps to make our software supply chain more secure, and unified our approaches across the federal civilian and national security systems, drawing best practices from both sides.

Then, as we responded to SolarWinds, Colonial Pipeline was hit by a ransomware attack in May of 2021. People trying to get gas in Virginia and North Carolina were most impacted, but it showed all Americans how a cyberattack could stop them from getting to work and school and could stop them from heating their homes.

Now, here we have a company that's part of our nation's critical infrastructure, privately-owned, as much of our critical infrastructure is, and definitely not the only vulnerable operator out there. We needed a new way to incentivize baseline cybersecurity strategy.

Those standards that we needed to apply had to be stronger building codes, if you will. A voluntary-only approach was clearly not sufficient to meet the growing threat. So, TSA created a sensible regulatory mandate for stronger cybersecurity and incident reporting for pipelines. They worked with the private sector to provide flexibility in achieving these goals, with a focus on performance, not paperwork. And their interagency partners expanded that effort by creating cross-sector cybersecurity performance goals that applied to every industry.

These actions were critical and they were far-sighted but they were still reactive, still incident-driven, the way cybersecurity had always been done. Reacting, however, will never get us to where we need to be. That's why this administration moved quickly to a proactive approach, one that takes the initiative from our adversaries by adopting a strategy not based on a single threat but on securing the very foundation of the digital world.

This is also where the Office of the National Cyber Director comes into the picture. As a brief aside, the path to creating this organization was winding, wasn't it, Mark? The Solarium Report launched on the 11th of March, 2020, just as the world was shutting down for the pandemic. The authorizing legislation squeaked through as one of the last acts of the 116th Congress, and we're all glad it worked out.

Now, Chris Inglis came on board in the summer of 2021, got funding by the fall, and staffed up over the winter, building out a great team one professional at a time. Now, from day one, by law and by leadership, this organization set a course focused on collaboration, building relationships across the interagency, with state, local, tribal, and territorial partners, with the private sector, civil society, academia, and all of our allies abroad.

The perspectives of these partners were front of mind as the team collaboratively developed a National Cybersecurity Strategy, which was published in March of 2023. Now, the drafters realized that without a clear, affirmative vision, the focus would be entirely on incident response, putting out fires as quickly as possible. That's a losing proposition.

We had to get to the foundation, to the code, the building code, and, in some cases, actual lines of code. So our approach started by laying out an affirmative vision for cyberspace, recognizing that cybersecurity enables literally everything in our increasingly digital world.

It laid out two foundational and fundamental shifts that were needed to make that affirmative vision real. First, rebalancing the responsibility to defend cyberspace towards the most capable organizations. And second, incentivizing long-term investments in cybersecurity and resilience.

Now, with the full implementation of these shifts, we can get all the cities in our digital world up to code and keep them there. Now, while everyone has a role to play in this work, it's on the federal government and the key technology companies to lead.

And we've acted on that responsibility. We've elevated ransomware as a national security issue, standing up a new cybersecurity section at the Department of Justice, the Counter-Ransomware Initiative launched by our friends at the National Security Council, which dozens of countries have joined, by the way. International cooperation was key to operations like the takedown of the Hive ransomware group.

And under the Cybersecurity and Infrastructure Security Agency, or CISA, pre-ransomware notifications started in 2023, and we've provided over 3,300 specific warnings to organizations like school districts and hospitals, alerting them to potential ransomware activities impacting their networks and helping them to prevent oncoming attacks.

Next, cybersecurity intelligence-sharing has reached new heights over the last few years. You've seen this in the run-up to Russia's unprovoked, illegal invasion of the Ukraine and around the danger posed by the People's Republic of China military units, pre-positioning themselves on our critical infrastructure. We are continuing to improve to get actionable intelligence out to cyber defenders on the frontlines, in the federal government and outside the federal government.

We're also being active on emerging threats, like the potential of a cryptographically relevant quantum computer to disrupt how we securely move sensitive information on the Internet. Here, the federal government is leading the way on assessing risks and prioritizing the development of quantum-resistant cryptographic algorithms.

On the private sector side, we have also driven progress. More than 260 tech companies and counting have joined CISA's Secure by Design pledge, a commitment to adopt elements of the model-building code, if you will, to reduce software vulnerabilities before they reach the market.

Industry partnerships, like the National Security Agency's Cybersecurity Collaboration Center and CISA's Joint Cyber Defense Collaborative, empower cybersecurity companies to better protect their customers, and they were key to the ransomware work that I just mentioned. These are some of the teams' accomplishments, and they are primarily a credit to our partners in the government and in the private sector.

Now, how does the Office of the National Cyber Director help? Well, we coordinate on cybersecurity strategy, policy, and implementation. And we've covered the strategy. Now let's take a look at policy and implementation.

It starts with collaboration and listening. Now, consider the 100 key initiatives in the National Cybersecurity Implementation Plan, designed collaboratively with the two dozen agency partners that lead them, including agencies that manage risk for each part of the economy, from agriculture to energy to telecommunications.

It means transparency. We listen to partners and the public, and we've published detailed reports for our stakeholders to review our progress.

It means accountability. Our "Report on the Cybersecurity Posture of the United States" gives a clear accounting of how we perform against the goals and the deadlines that are listed in the National Cybersecurity Implementation Plan. And it means advocating for resources.

We all know that strategy without funding is mere rhetoric. So, from its first days, the Office of the National Cyber Director has partnered with the Office of Management and Budget to set cyber funding priorities for each federal department and agency.

All of our collaborative work coordinating strategy, policy, and implementation reflects our commitment to coherence, to ensuring that agencies' cyber actions are unified. Now, we advance government-wide coherence by driving a virtuous cycle where strategy informs policy, which informs the implementation plan and resourcing, and measured outcomes from the next version of the plan.

The United States is also forging coherence globally. Think of digital solidarity, the vision outlined by Ambassador Nate Fick in the State Department's International Cyber Strategy. It's all about outlining a shared vision for cyberspace with our allies and our partners.

A contemporary example, I was just in the United Kingdom last week, discussing issues like cyber-enabled fraud, a national challenge, an international challenge, and a challenge that the United Kingdom has taken a leadership role on.

Now, there are a few areas, however, where the Office of the National Cyber Director is not only coordinating, but is leading the charge. We have taken on some of the hardest long-term problems in cybersecurity, and we are driving progress.

Whether they're hard technically because a solution hasn't been figured out, hard to deploy because of the sheer numbers of players involved, or hard because competing interests must be balanced, these are issues that many of us have talked about for years and sometimes decades. These problems each needed a dedicated leader, and our office was eager to take them on.

Let me share a bit of our progress. In February, our office released a report entitled "Back to the Building Blocks" for our technical systems. It shined a light on memory safety vulnerabilities that have plagued the digital ecosystem for more than three decades.

These are tied to the use of unsafe coding languages, and they account for a staggering amount of intrusions. The report called on technology manufacturers to prevent entire classes of vulnerabilities from entering the digital ecosystem by adopting memory-safe programming languages.

The report on the building blocks also called on the research community to focus on software metrology or measurability to enable the development of better diagnostics that measure cybersecurity quality.

Our focus on these building blocks of cyberspace has been influential in several ways. It galvanized new ways of thinking about how to improve safety for commercial products and services produced around the world.

It spurred development for better diagnostics for cybersecurity quality. It inspired other countries, which have sought our help to emulate this engineering forward approach to policymaking. And the team's approach is leading to increased government investment.

Recently, the Defense Department, specifically DARPA, announced an investment of roughly a quarter of a billion dollars to work on technical solutions aligned with Back to the Building Blocks. That report has been influential.

Next, let's take a look at a deployment challenge, securing the routing of information across the Internet to ensure that it goes exactly where it should, without bad actors intercepting it. This requires adopting border gateway protocol solutions. The model building code for this has long existed.

It starts with registering Internet addresses under an agreement to enable more secure Resource Public Key Infrastructure, or RPKI, services. But this solution was not being implemented because of the sheer number of network users and the lack of sufficient incentives to act.

Since the United States government is the largest owner of address space, we've worked with the Department of Commerce to ensure that we led the way. A year ago, only a quarter of federal civilian Internet address space was able to use RPKI.

Now, after spearheading an interagency campaign, roughly 90 percent is covered under an agreement that will enable RPKI services. And we built deep public private collaboration to guide network operators in this work – certainly, more work to do, but we are on a remarkable trajectory.

Next, we've developed options to address the hard legal problem of software liability. Now, this is a tough, tough challenge with enormous consequences for IT companies, as well as for American businesses and consumers. Liability is a key lever for aligning the incentives across these stakeholders, and that alignment takes real work to achieve.

So, we pulled together legal researchers for a software liability forum at the White House. Then we developed a range of detailed potential policy approaches that are ready for the incoming administration and Congress to consider.

The next hard problem is duplicative federal regulation. This is an issue our partners in industry and critical infrastructure have long said gets in the way of their ability to do business and to focus on cybersecurity. To learn more, we put out a request for information, or RFI, and we got detailed responses from companies in every sector of critical infrastructure.

One respondent actually told us that a staggering 30 to 50 percent of CISO's time is spent on compliance – not cybersecurity, but compliance alone. Armed with industry's call to streamline, we worked with Congress to write bipartisan legislation that would bring all stakeholders, including independent regulators, to the table to advance the regulatory harmonization and reciprocity that industries need.

Many of us were disappointed that this has not become law yet, but we have laid the groundwork for the next administration and Congress to do the right thing for our partners in the private sector. They understand that to undo regulatory harm, we need regulatory harmonization. Building codes should not be in conflict with each other.

Now, the final hard problem I want to cover today is fulfilling the need for cyber talent. Everywhere I go, whether I'm talking to state or local government leaders, small or large businesses, or anyone leading critical infrastructure, they all tell me they need more cyber talent.

Today, there are nearly 500,000 open cyber jobs in this great nation. So, we need to reach more communities, and we need to invite them to see themselves in cyber.

In community colleges, technical colleges, historically black colleges and universities, and other four-year institutions, in Pennsylvania coal country, in rural Mississippi, farming communities in Wisconsin, and on both coasts, in all of the dozen states that I visited, I meet people eager to have good-paying, meaningful careers in cyber.

These visits have helped implement the nation's first-ever comprehensive Cyber Workforce and Education Strategy. Under this strategy, we have employers, educational institutions, non-profits, and all levels of government singing from the same song sheet.

More than 180 of these organizations have made commitments following the course that we've laid out. Taken together, they have pledged to hire more than 35,000 workers; $110 million pledged to expand training and education. And again, the federal government is leading by example. With our partners at the Office of Personnel Management and OMB, we're moving federal employee and contractor hiring from a focus on college degrees to a focus on what we're really after – skills.

Those are some of the hard problems that we've been working on, but many more remain, so it's good to have the Office of the National Cyber Director team at the ready.

To recap, in the last four years, we have fought fires, then taken a proactive posture to defending cyberspace; brought greater coherence to federal and global efforts; gotten tech companies to step up on cybersecurity; and taken on some of the hardest problems that have long crippled our ability as a nation to stay secure.

That's progress. Again, there is still a mighty long way to go, but we made progress in ONCD. We'll continue to do so because of how we work and the unique capabilities that we have developed. Our policy-making capability means the team can look at the biggest challenges holistically, gather and analyze input from all stakeholders, and forge real, actionable consensus on the way forward.

Our implementation capability means this team can deliver against the strategies that we create, with a nimble cadence of action, review, revision, and more action. The proof, the number of mission partners volunteering to lead implementation initiatives grew from year one to year two of our national strategy.

Our reporting capability makes us truly transparent and accountable. We encourage you all and the public to read about what's getting done and where we're falling short, and you can do that at WhiteHouse.gov/ONCD.

And that brings me to the last capability that I want to highlight, ONCD's practiced ability to build partnerships that execute on mission. It's based on the trust that we've built – I should have said, the trust that we have earned over these four years, and it's perhaps the most valuable capability of all.

Unlike more traditional domains of conflict – land, sea, air, and space – cyber defense is a shared responsibility. Our nation's security and economic prosperity depend on close collaboration with partners, including the private sector and our allies.

We need public-private partnerships to continue accelerating the sharing of cyber threat intelligence and best practices, and to move from simply sharing information to operating joint cyber defensive activities. And partnerships are needed to solve even more of the hardest problems, like the challenges posed by A.I. and quantum computing.

Now, I'm particularly energized by the evolving partnerships with the state, local, tribal, and territorial governments, the SLTTs. We have worked closely with them, sharing information about federal resources that can help them build resilience, like free cybersecurity tools for K-12 school districts and public libraries.

I want to recognize the smallest state, Rhode Island, for being the first state to commit to making every one of its public schools and 136,000 students more safe – more cyber safe by using Protective Domain Name Service, PDNS. We strongly encourage every state to follow the lead of our smallest state, Rhode Island, in adopting this highly effective, no maintenance tool fully funded by the federal government.

Now, my time traveling across the country, including to host many roundtables with K-12 school leaders as well as with cyber employers and students, showcased the unique convening authority of the White House. Now, because of these events, hundreds of educational leaders know more about how to access the resources that they need. They are now more closely connected with our mission partners at CISA and the FBI, who provide day-to-day support in their community.

So federal unity of effort isn't only real here in Washington, D.C., it is real to the people who educate our children and to more and more people on the cyber frontlines across sectors nationwide. Because of the ONCD team and our great mission partners. That's why.

So in four years, while our office is small and we are close to reaching that full compliment of 85 people, we are powerful and we are making an impact. We have come a long, long way since we were an army of one. The team is ready and able to do more, and it needs to do more because cyberspace will continue to grow.

By adopting and enforcing building codes, America's cities and towns could continue to grow ever bigger and more beautiful while conflagrations decline. Working together, we, all of us, can create the same future for our cyber America. We can make it safe and functional, and more. A place where people work and play, connect and create. A place of innovation and opportunity for all.

Getting there is our mission, and that mission will endure. Looking ahead, there are two things that I am certain of. One, our digital foundation is getting stronger, and a proactive approach will continue to help protect our great nation. And two, the ONCD team will serve the American people in the Trump administration and beyond with dedication and excellence.

My ONCD colleagues don't know any other way. Their professionalism knows no bounds. I've been proud and will remain proud to call them shipmates. It has been a tremendous honor to serve as the National Cyber Director, and a greater privilege to have worked alongside all of our partners.

Thank you.

(APPLAUSE)

MONTGOMERY: Thanks, Harry. All right, that was the easy part.

COKER: Yeah.

(LAUGHTER)

MONTGOMERY: All right. All right. So first, that was a great discussion, and I'm glad I saw Drenan is here, and the shoutout to Chris Inglis and Kemba Walden as well. And as you said, you have a great team.

But I think one of the most important events you participated in was last January, January 31st, you, Director Chris Wray from the FBI, then-Cyber Command Commander General Paul Nakasone, and CISA Director Jen Easterly, testified in front of the China Select Committee about the growing threat of Chinese intellectual property theft, espionage, and, at that point, really focused on what we call preparation – operational preparation of the battlefield. The – and I think simultaneously, Director Wray revealed the Salt [sic, Volt] Typhoon case.

Can you kind of take us – so it's a year later now – take us through, when you sit back and think why ONCD's relevant, why the federal government has such a strong role in cybersecurity. What is the threat to us, both, you know, nation-state, and particularly China, but also criminal?

COKER: Yeah. Well, I will not forget that date, 31 January, 2024, when the four of us testified before that House subcommittee, and one of our great cyber partners, the former Representative Green and his subcommittee.

One of the key points – and there were many – for that day is making the American public aware of the unacceptable risk posed by the People's Republic of China. It's too often overlooked, but every one of us needs to recognize the threat posed by the PRC, and every one of us need to ensure that the federal government and its mission partners are addressing that threat. It's too easy to become complacent while adversaries are prepositioning themselves on our critical infrastructure. We take it for granted that that critical infrastructure is there to serve us, to help us maintain a quality of life, and it is there until it's not. But when an adversary, a nation-state or a malicious cyber criminal puts us at unacceptable risk, we need to take action.

And so that was the big thing: making sure that the American public is aware of the threats posed by these nation-state and non-nation-state actors that would do us ill will.

Now fortunately, the National Cybersecurity Strategy is threat- and technology-agnostic. The relationship to the building codes, that strategy is a building code, and at one point in the remarks I talked about how the building codes are effective only when they are adhered to.

The same applies to cybersecurity. We have a strong National Cybersecurity Strategy. We have strong policies in place. We need to incentivize every entity, individual and organizational, public, private sector as well, to implement those building codes. When we do that, we will be safer, and we will be more prosperous. But frankly, we have work to do on incentivizing entities to do the right thing.

MONTGOMERY: Yeah, I couldn't agree with you more on China. You know, the – since Vo- – Salt [sic, Volt] Typhoon, we've announced Volt [sic, Salt] Typhoon, which was a significant espionage case against our telecommunications industry, and Flax Typhoon, which is probably a mix of espionage and intellectual property theft against a series of companies, including the Department of Treasury systems.

China – I think you're absolutely right – does not feel constrained at all about operating in our systems, and if you think – I get that espionage is handled separately, but this operational preparation of the battlefield – if I were to go to any other warfare area, you know, as I – you and I – and I should have mentioned you're a career Navy officer, as well. It's – obviously shows you where the – how the Navy sits with the two of us.

But both of us would've, in a previous life, said operational preparation of the battlefield in a submarine context or an air context, that would be steps leading to war. But you know, China appears to feel that they can operate in here, you know, could – you – without punish – without fear of punishment. How do you think we message properly to China about this?

COKER: In multiple ways. We do have to deter the People's Republic of China and others that would do us ill will that they cannot operate freely, and we say we're at unacceptable risk. Well, unacceptable means you can't do it. So we have to get them out of there, and we have been working for quite some time to do that. But again, that's almost when the smoke has started. We need to get to the pre-smoke, if you will.

We have to use every tool in our national power – diplomatic, economic, intelligence, coalitions – to have like-minded nations – because the PRC is operating against us, no nation should feel safe – to deter the PRC from doing this.

And I will say, just speaking frankly, we have to improve on that deterrence. That proof is there, and we have to do a better job at deterring the PRC.

MONTGOMERY: I love how you – you know, your building code analogies about resilience, and that – and so I – I do think it's both things you said there. It's, we have to improve deterrence by cost imposition. That's both a capability and a political process. It's not the NCD's; it's a – the president and the national advisor's. I get that. But then the one where you're really focused: deterrence by denial, improving our ability to both at a corporate level, an infrastructure entity level, and a federal level, prevent Chinese penetrations.

And of course, you said it right. That gets you the National Cybersecurity Strategy is threat-agnostic, because if you're better against Chinese penetrations, you'll be better against criminal ransomware penetrations. You'll be better against Russian penetrations, Iranian penetrations, North Korean malfeasance. So you're absolutely right. The strategy's threat-agnostic but is necessary for every threat.

COKER: It is, it is. And then also, you mentioned a phrase, impose costs. If that strategy is adhered to, that will impose costs on malicious cyber actors, nation-state or non-nation-states.

MONTGOMERY: You know, I like that, and let's talk about the strategy. First of all, again, you know, Kemba Walden and Chris Inglis, your predecessors, deserve a lot of credit, but so does your current team for the implementation strategies and, you know– strategies that are just doorstops, you know, they proliferate throughout the government, and they're of marginal value. I love the fact that you took it as an implement– and have now done implementation versions on it, you know, to try to get it done.

I think one of the things that when I read through it is most clear is that resources are required. And you said a line, I think, Frank Cilluffo, one of our commissioners used to say strategy without resources is rhetoric, and you know, you – I think you agree with that from your remarks.

You guys had a unique opportunity partnering with the Office of Management and Budget. Can you describe that a little bit and describe how you think that works going forward?

COKER: Yeah. Yeah, thanks. The relationship with the Office of Management and Budget is key. OMB controls the purse strings, if you will, and to their credit, OMB recognized that the subject matter expertise from a technical perspective and a policy perspective when it comes to cybersecurity is within ONCD. OMB did what I always want organizations to do: leverage the core competencies of your partners. They saw our core competency. They brought us in and asked us to work with them on prioritizing cybersecurity priorities for the department's agencies and the federal government, which we have done. That's been a strong partnership.

To no one's surprise, those priorities are in alignment with the national cybersecurity and the implementation plan, which is great.

Now – and I also want to pass along that – I mentioned in the remarks, and this does go to resources, the Executive Order 14028. I was on a video call with a CISO from a major agency a number of months ago and the CISO thanked us, and I had to pass that gratitude along to the National Security Council, who was the impetus behind Executive Order 14028.

That CISO said they – when they walk up to their chief executive's office now, they carry that 14028, and said this is the nation's priority on cybersecurity, are you going to fund it? And it has made a difference when it's put in that light.

It gets to the challenge that many cybersecurity professionals in and outside of the government face in that organizations too often are focused on what I'll call their main line of business without realizing that their main line of business does not happen without cybersecurity, it is foundational, and it needs to be treated as such.

MONTGOMERY: Yeah, I think that's a fantastic point. You know, the – I think you do have to give a lot of credit to the OMB Director, Shalanda Young. She...

COKER: Absolutely.

MONTGOMERY: ... I mean, she did something that federal executives seldom do, which is, you know, give away some responsibilities to your team. Now, it helped that you had selected a partner of hers from the Senate Appropriations Committee to be your lead, so that you're able to get with Drenan Dudley, that you're able to have some trust there. But that's the kind of trust that leads to success.

I'll tell you, at the commission, we studied the 15 years before the Biden administration, looking back for times when OMB passed back budgets because of insufficient investments in cybersecurity. And the answer is they didn't. They just didn't have the expertise, the time, you know? The – that's not where OMB was focused.

So, like you said, having the trust in you to have you do that – and I really hope, of – there's a lot of interesting side deals you had as NCD. That's one that is really important that it carries over into the next administration.

COKER: It is, and a deal like that is possible for an organization to share or give away some of their responsibilities and authority, share, when that organization is professional, they are mature, they are confident, and they can do that, they can provide that trust.

Those that don't want to leverage their partners are not – are not as confident and perhaps not as competent when it comes to leadership. That was not the case with OMB.

MONTGOMERY: And I think, as you look back, there's going to be – you know, there's two types of budgets, and on one of them, there's just such clear success, which is the funding of the dot-gov. You – we now see it several years in a row now over $13 billion for the dot-gov, which is about the same, you know, for perspective. The dot-mil is about $13 billion on cybersecurity – you know, cybersecurity issues. It – and we know they're about the same size at the unclassified level – you know, the – on the same classified system. And so I have a strong belief that it's been successful.

And you're right, Cabinet – look, the Secretary of Agriculture, five years ago, you know, cybersecurity was not job one, you know? Ferreting out, like, mad cow disease, that was – that's job one, and I get it. I don't want mad cow disease.

(LAUGHTER)

But it's a – it – you know, at some point, he or she has to understand they can't find mad cow disease if they're – none of their IT systems function.

COKER: Agree. And so that's part of the educational process. When I talked about 31 January last year, making the American public [aware] of the threats posed to our critical infrastructure, that happens because of our insufficient cybersecurity posture. And we have to realize what is at risk.

MONTGOMERY: You know, I think the other area of budgeting and that – one where there's been improvements but there's still – I think you've left room for your – for the next team as they come in, and that's the sector risk management funding.

I think some sector risk – some sectors – and, you know, I always put – I'm probably condemning them to a massive attack next week, but the energy sector and the Department of Energy and their CESER, that's really well-funded.

And – but you look across other federal agencies and – you know, Department of Education, Department of Agriculture – you really worry about do their – are they getting a – enough funding to do their job? And you know the numbers, they're pretty low.

I think that that's – if there was an area I'd keep putting a lean on, you know, as you – as you create that package for your relief, it's – it's a – getting that sector risk management, get everyone on Energy's level. That's hard though. That money – that significant money, that's 15 – or in that case, $100 million. I don't know that all federal agencies get that just yet. I do think you've convinced them on the dot-gov. I think the sector risk management agencies the next big hurdle.

COKER: I agree, and it goes back to what we've previously said – that main line of business does not happen without cybersecurity. The nation is in a tough budget situation. I get that, and I support making progress towards reducing the deficit, but we have to prioritize cybersecurity within our current budgets. We can do that. It's non-traditional for some that are in those departments and agencies to have cybersecurity professionals move up in the prioritization, but that is what needs to happen.

MONTGOMERY: That's great, thank you. And budget's a tough one. A better issue, one you and I love together – you know, we both have a real passion for is workforce.

COKER: Yes.

MONTGOMERY: The – you've – you know, I have a longstanding love affair with the CyberCorps Scholarship for Service program. You stepped in and really grabbed the bull by the horns in – as NCD and really got the first Cyber Workforce and Education Strategy, as you mentioned, out.

As you look at it now, where are the successes and where kind of are the opportunities for more work in this area, which we both think is probably key to success?

COKER: Yeah. The successes – so many of the successes across the board have to do with making people aware of the opportunities. And what we've worked with OPM on and our – and CISA and FBI, getting out around the country, making sure that everyday Americans, those real Americans that those in Washington, D.C. don't interact with much, understand that cybersecurity, cyber, provides good-paying jobs and meaningful careers.

Cyber Strategies and Successes: A Conversation with National Cyber Director Harry Coker, Jr

January 7, 2025
Featuring Harry Coker, Jr. and RADM (Ret.) Mark Montgomery

We were in – in coal country in Pennsylvania a number of months ago, talking with a young person about how they got interested in cybersecurity. And the individual had worked at a 911 call center, and that person took a call from what they said – well, an elderly lady. She was a widow. And she was broken down because someone had just defrauded her of her and her late husband's life savings.

And it struck that young 911 call operator so much that he vectored off – he was already helping people, doing a public service in 911, which is vitally important – but that person decided that they wanted to go into cybersecurity because they did not want that to happen to anyone else.

So we need to make sure that individuals know it's a good-paying job. It is public service, even in the private sector. I talked about how cybersecurity is a shared responsibility.

Our private sector does a public service in cybersecurity, and we can do that. Those of us who care enough about others, who want to serve others, you can do that in cybersecurity. So, making people aware of the opportunities there.

It used to be where people thought cyber professionals were just geeks doing code and not doing anything else. You need not be a master of technology. So, the opportunities are there.

We need to go to places like, again, coal country in Pennsylvania, and Jackson, Mississippi where I was a month and a half ago, and let those folks know that there are opportunities there to contribute, not just to their immediate family's livelihood, but to their community and to their nation. They can do that. So, that's one, making people aware of the opportunities.

Number two, we want to increase the number of pathways into cyber careers. Increase. We don't want to take away any pathways. One way we are increasing pathways is to do away with unnecessary, in many cases – not all cases, unnecessary four-year college degrees.

I imagine most of us know some young and not-so-young people who have some skills that they developed outside of a four-year college university and can be applied. What's near and dear to me, and probably you and General Gibson, just right up the road at Fort Meade, where we have an awful lot of enlisted members on the front lines of cyber every day. While many of them do have four-year degrees, many of them do not.

The way we were headed with these four-year degree requirements, which by the way are proxies for skill, OK, we were eliminating many of those enlisted members that are on the front lines of cyber every day, demonstrating their values by contributing to our nation's cybersecurity.

Well, when we do away with the four-year college degree requirement, we expand our talent pool, and that's what we need to do more of.

MONTGOMERY: Yeah, I love the push you've had for skills-based hiring requirements as opposed to degree-based. And I think that's going to go a long way. I think one of the big wins is, in a place where there's great bipartisan support, is in this workforce.

I think the Pivot Act by Representative Green, who's chaired, as you mentioned earlier, the chairman of the House Homeland Security Committee, it's a cyber – it's a CyberCorps for vocational and community college skills-based requirements.

I think we'll get people faster. It has the same scholarship for service intent where we pay for a year or two of you to go to community college or vocational training, and you owe us, you owe the government that year or two. I think your proselytizing about that has, really, you know, has sunk in, and you're going to see a large hire.

The federal government part of cybersecurity workforce, and one of your two big efforts there, is really going to win from that.

COKER: It is. It's going to happen because it makes too much sense. We want people with skills working. So, the skills-based approach is the way to go. And we can develop those skills well short of four years.

And, you know, I want to be clear. We are not saying don't go to colleges and universities for four-year degrees. We are saying let's expand the pathway, expand the talent pool.

Many Americans don't have the time or the means to go to college for four years, but they can do it for two years or less. We're expanding the avenues of coming into a cyber career.

MONTGOMERY: And you're right. The government hasn't given up on the bachelors or the masters or even the doctorate. I saw there's a small change to the CyberCorps legislation coming through now to allow to train people for doctorates if they go teach at a CyberCorps university, because one of the things we're finding is we actually don't have enough Ph.D.s in cybersecurity policy right now because it's so lucrative to leave academia.

So, by having these extended scholarships, someone then owes a significant amount of time. You know, that's how the Navy tricked you and I into long and fulsome careers. So, yeah, I – I'm a big fan. I think you've had the exact right balance in that that that's gotten us to this point.

I know we're running a little short on time but there's two last issues I want to talk about – one state and local government, because I think one of the areas that's really blossomed over the last four years due to the interest of the national cyber director, but also Congress's Bipartisan Infrastructure Act which actually set aside about a billion dollars for state and local to attack this issue.

What's your take on that? And where do you think that can go moving forward? And how have we done with the state and local entities?

COKER: We've made progress. I'll just talk to where it needs to go. We need to do a better job of supporting state, local, tribal, and territorial entities, SLTTs. Our adversaries recognize that's a soft underbelly of America's cybersecurity posture. And as any capable adversary will do, they'll go to the weak spots. And right now, SLTT's represent weak spots for us.

The federal government has to figure out how to better support SLTTs. It's a challenging, challenging area. I mentioned the rural places around the country that we have been to. Those municipalities are protecting schools and libraries and hospitals and houses of faith.

And while some of those may not be of significant military value, if an adversary were to inflict what I'll call "cyber terrorism" on them, societal panic that will cause the local communities to lose faith in their government, which we do not want or need or deserve.

So, we have to figure out how to better support SLTTs. It's going to be some means of shared services. It's going to be some means of upscaling defense to the meet – to the ways that offense has been scaled. But it's a challenge area that we have to figure out.

MONTGOMERY: Now, I think you're right. I think you guys have made real headway here. I think that money will expire in about 18 months. So, you know, but the – when you think about the most vulnerable utilities and assets we have, rural hospitals, rural water supply, almost all K-12 education systems, they could really benefit from this.

And so, I'm glad you're working it. And one of the things we'll be pushing this year is a virtual CISO, fractional CISO, some pilot programs the idea that like a rural hospital can't afford a CISO 365, but they can sure use one just after a ransomware hits.

And the person comes in, and for a fractional pay fixes the problem. And the smart hospital administrator goes, "Well, that saved my bacon," because most rural hospitals can probably operate for four to six weeks float then they're out of business. In other words, if they're not back up and running fully accepting funds back in because they're processing things, they won't exist.

The smart administrator will say, "You know, I think I'm going to invite that person for a fractional visit before my next attack. And maybe my next attack won't occur." So, I'm really excited. And that's this is spurned by the thoughts from the cybersecurity assessment – your national strategy and ongoing assessments.

Let me – so we're at the – near the end of this discussion. We're also near the end of the administration. For the new team coming in, I – you know, you framed it right. When the Biden team came in, they had SolarWinds right in the windshield, you couldn't avoid it. NCD was going to be a team of one in about five months.

COKER: Yep.

MONTGOMERY: I wouldn't say the – my personal opinion, I'm not sure the administration accelerated that effort, but we'll let it go. As a result, there was a very robust National Security Council presence in cyber – defensive cybersecurity.

As you look forward to the next administration, what's your recommendation on – now that you have this robust NCD that's going to turn over, you know, 40 or more, you know, people in hand at the time, what's your recommendation for kind of, like, the lay of the land in White House and agency management of cyber defense?

COKER: So, kind of touched on it in the remarks and – but, again, at the outset, it was a small team at ONCD. We took on as much as we were capable of taking on, given the resources. Since then, the resources have expanded, and we have taken on additional responsibility. There is still more that we can and should do in the cybersecurity landscape with regards to planning and response, for example. That's an area where we ought to try to take on more responsibility.

Frankly, I also believe that our relationship with the OMB can grow and be strengthened. And I'm not going to dance around things – it's good to give budget guidance. We need to give budget direction when it comes to cybersecurity.

I would love for the incoming administration or any in – in – administration to recognize the priority of cybersecurity. It's a responsibility that every department and agency needs to stand up to. We need to give more of than guidance when it comes to cybersecurity budget.

MONTGOMERY: I think the Chinese are helping you on that routinely.

(LAUGHTER)

So I – one other thing I would recommend is that the – I think we're at the point now where we have a mature, scalable NCD, a National – Office of National Cyber Director. As the National Security Council is stood up, I think its Cyber Division should revert to a traditional form of being really responsible for offensive systems, working with State Department on the international aspects, and then when an issue rises to a really high national security level, that they're involved in the management of it.

But if I could go back in time, the one thing that – he now works for you, but he worked with us in a time, Nick Leiserson – we probably traded away too much of the NCD's policy management role, and hopefully that's something a President can give the NCD, and give you management of the national critical infrastructure protection mission in a way that I think – you know, from a cybersecurity point of view, that – a way I think that would be beneficial in allowing NSC to run more fluidly too, I think.

I think that's probably where this team's headed but I have no idea. I hope that they look at the work and the journey you've been on and say the Office of the National Cyber Director is in a position now to be the coach of the cybersecurity team. You've got CISA as a quarterback, you've got a lot of federal agencies out there doing their job, but at this point, I think they can empower you with that in a way that probably didn't exist in January of 2021 when they took over.

So I want to thank you very much for your service, thank you for taking the time here, and really thank our audience for being here on a rough weather day. Thank you, sir.

COKER: Thank you.

(APPLAUSE)

END