

Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TITLE TO RECEIVE TESTIMONY ON UNITED STATES
CYBER COMMAND IN REVIEW OF THE DEFENSE
AUTHORIZATION REQUEST
FOR FISCAL YEAR 2026 AND THE FUTURE YEARS
DEFENSE PROGRAM

Wednesday, April 9, 2025

Washington, D.C.

ALDERSON COURT REPORTING
1029 VERMONT AVE, NW
10TH FLOOR
WASHINGTON, DC 20005
(202) 289-2260
www.aldersonreporting.com

1 HEARING TITLE TO RECEIVE TESTIMONY ON UNITED STATES CYBER
2 COMMAND IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST
3 FOR FISCAL YEAR 2026 AND THE FUTURE YEARS
4 DEFENSE PROGRAM

5
6 Wednesday, April 9, 2025

7
8 U.S. Senate

9 Subcommittee on Cybersecurity

10 Committee on Armed Services

11 Washington, D.C.

12
13 The committee met, pursuant to notice, at 3:40 p.m. in
14 Room SD-G50, Dirksen Senate Office Building, Hon. Mike
15 Rounds, chairman of the subcommittee, presiding.

16 Committee Members Present: Senators Rounds
17 [presiding], Rosen, King, and Reed.

1 OPENING STATEMENT OF HON. MIKE ROUNDS, U.S. SENATOR
2 FROM SOUTH DAKOTA

3 Senator Rounds: Good afternoon. I'd like to express
4 my gratitude to Lieutenant General Hartman for his
5 attendance at today's hearing.

6 Before I proceed any further, I want to acknowledge the
7 incredible momentum set by General Haugh and the strategic
8 transformation needed to meet the evolving threats of today
9 and the emerging challenges of tomorrow in cyberspace.
10 General Haugh was a strong leader with a deep knowledge of
11 the art and science of cyber warfare, hard earned over three
12 decades of service to our country.

13 Men and women capable of leading the National Security
14 Agency and the United States Cyber Command are in short
15 supply. Such leaders require years of experience to develop
16 with deliberate and dedicated career focus. To put it more
17 directly, we do not have enough of these types of leaders,
18 and a loss of any one of them without strong justification
19 is disappointing. The departure of General Haugh is a loss
20 for our nation, but will be a tremendous gain for any
21 private or public entity where he decides to lend his
22 expertise and leadership. I wish him God speed.

23 That said, as our adversaries watch this hearing, it
24 will be clear, that no matter the scenario, our cyber
25 mission forces are ready. Lieutenant General Hartman's

1 presence is more than just an annual congressional activity.
2 His presence is more than just a general annual
3 congressional activity. It shows the strength and
4 resiliency of the cyber mission force. It is a testament to
5 how much this command has matured since its inception in
6 2009, and the steadfast nature of our military, civilian and
7 uniformed, to step up and fight when the nation needs them.

8 It also reflects the absolute importance of the dual
9 hat arrangement, in the face of unexpected change there
10 remains tight integration of cyber and intelligence
11 operations, thanks to alignment under a single leader. Such
12 an arrangement remains paramount in future decisions of
13 General Haugh's formal successor.

14 I have had the pleasure of working with Lieutenant
15 General Hartman in his prior role as Deputy Commander of the
16 United States Cyber Command, and I am confident in his
17 ability to lead these organizations through this transition,
18 maintaining the combat capability of a force that operates
19 in an environment of constant change. He is one of the few,
20 with a strong understanding of this domain, built over
21 decades of experience.

22 The importance of the cyber domain cannot be
23 overstated. Our adversaries understand the dynamic and
24 permeable nature of cyberspace and have clearly demonstrated
25 their intent to exploit it to their advantage. General

1 Hartman, as we discussed in detail during our closed
2 session, the threats our nation faces in the cyber domain
3 have only intensified since we last convened for an update
4 from CYBERCOM a year ago.

5 The detection of additional Chinese advanced persistent
6 threat groups throughout the past year has reinforced both
7 the determination of our adversaries to own this domain, and
8 their technical capability to do so. With the release of
9 the Chinese generative artificial intelligence, large
10 language model or DeepSeek-R1, earlier this year,
11 competitive advantage will now be measured in weeks and
12 months, not years. Our cyber mission force must be ready
13 with training, technology, and operational structure to
14 deter and defend against this new reality.

15 I have been encouraged by the work the command has
16 conducted on CYBERCOM 2.0 in collaboration with the services
17 and the Assistant Secretary of Defense for cyber policy. I
18 want to hear what policy changes are needed to realize the
19 vision behind this effort. And while I understand the
20 implementation plan has not been delivered to Congress, our
21 adversaries are not waiting for our process to conclude.

22 I look forward to hearing more from you about the
23 efforts underway to implement CYBERCOM 2.0 and how you
24 intend to make sure the force is maturing, to conduct
25 persistent engagement in this competitive environment.

1 I will now recognize Ranking Member Reed, from the full
2 committee, at Senator Rosen's request, for opening remarks.

3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 STATEMENT OF HON. JACK REED, U.S. SENATOR FROM RHODE
2 ISLAND

3 Senator Reed: Thank you very much, Mr. Chairman, and
4 thank you Senator Rosen. I just want to take a moment to
5 recognize General Haugh for his 35 years of dedicated
6 service to this country and to the United States Air Force.

7 His sudden and inexplicable firing is disrespectful to
8 his service, but also disrespectful to every military member
9 in or out of uniform, and an indication that their service
10 and sacrifice is in no way respected by this administration.
11 The callous nature of the decision, the result of a meeting
12 with a partisan conspiracy theorist, not on any kind of
13 informed or experienced judgment, puts our security at grave
14 risk and cannot be tolerated or continued.

15 We salute a dedicated American for his service and
16 sacrifice and his family for standing with him and wish him
17 well. Thank you, Mr. Chairman.

18 Senator Rounds: Ranking Member Rosen.

19
20
21
22
23
24
25

1 STATEMENT OF HON. JACKY ROSEN, U.S. SENATOR FROM
2 NEVADA

3 Senator Rosen: Thank you, Chair Rounds, and thank you
4 Ranking Member Reed. Of course, this is such an important
5 hearing, and I appreciate General Hartman, our meetings that
6 we had yesterday and your team, all of your service, your
7 commitment to the mission and on the success, because that
8 means that we're all kept safe.

9 And you're also here on very short notice, as we've all
10 been talking about, and we appreciate that as well. And so,
11 I look forward to continuing our conversations and our
12 continued partnership to ensure that success.

13 And like my colleagues, I want to begin by addressing a
14 matter of significant concern, the sudden and inexplicable
15 firing of General Haugh, a trusted and dedicated Air Force
16 officer for over 34 years, a true patriot. His abrupt and
17 unjustified removal was conducted in the dead of night, with
18 absolutely no consultation with Congress, the full
19 committee, or this subcommittee.

20 And according to press reports, it was at the request
21 of a private individual outside of the government, outside
22 the chain of command, who has a long record of pedaling in
23 vicious conspiracy theories. This action compromises
24 CYBERCOM and the NSA ability to keep Americans safe.

25 United States faces major cyber threats from foreign

1 adversaries, China, Russia, Iran, near daily cyber-attacks
2 and our critical infrastructure. And at the same time, we
3 are engaged in ongoing operations against multiple threats
4 across the globe, from Russian aggression against Ukraine to
5 Iranian backed proxies in the Middle East and North Africa.

6 Given the dangers facing the U.S. and our troops, it is
7 inexplicable and unconscionable that the President would, at
8 the mere request of an online provocateur, remove the leader
9 of CYBERCOM, completely without cause and in doing so, risk
10 undermining vital intelligence operations.

11 Moreover, General Haugh has been a trusted leader. His
12 experience and expertise have been crucial in guiding and
13 shaping the efforts of U.S. Cyber Command and our overall
14 national defense posture. At a time when our adversaries
15 are constantly evolving their cyber capabilities, whether
16 it's from state actors like Russia, China, Iran, or North
17 Korea, or non-state actors with nefarious intent, leadership
18 continuity and clear vision are more critical than ever.

19 Cybersecurity and cyber operations are not and cannot
20 be a partisan issue. It is a national security imperative,
21 and the threat environment as we all know, continues to
22 intensify every single day. We must maintain experienced
23 leadership to counter the ever-evolving cyber challenges
24 facing our country. As members of this committee and the
25 full committee, we must demand clarity from the

1 administration about the rationale for this decision, and we
2 must not rest until we have answers and accountability from
3 both President Trump and Secretary Hegseth.

4 This afternoon though, our focus will be on our
5 nation's cyber capabilities and how Congress can help
6 support the critical work that CYBERCOM personnel do every
7 single day. I might say 24 hours a day, 24-7, 365.

8 And so, I look forward to hearing from General Hartman
9 and to discussing how we can meet our nation's challenge.
10 And today, in the future and over the course of this
11 congress, again, I know how much General Hartman you are
12 invested in the mission of CYBERCOM, how much you know about
13 it, your experience, your expertise and how invested you are
14 in the ongoing success in combating cyber threats going
15 forward. And I do look forward to working with you on that.
16 So, thank you, Mr. Chairman.

17 Senator Rounds: Thank you, Ranking Member Rosen. And
18 with that, Lieutenant General Hartman, welcome. Thank you
19 for your service. We thank your family as well for their
20 sacrifice, and there's a lot of things that you literally
21 don't get an opportunity to share with the American public
22 because of the type of responsibilities that you have. But
23 today, you have an opportunity to share with the American
24 people and with this committee a little bit about what you
25 are doing. And we welcome your opening remarks at this

1 time, sir.

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 STATEMENT OF LIEUTENANT GENERAL WILLIAM J. HARTMAN,
2 USA ACTING COMMANDER, UNITED STATES CYBER COMMAND/ ACTING
3 DIRECTOR, NATIONAL SECURITY AGENCY/ ACTING CHIEF, CENTRAL
4 SECURITY SERVICE

5 General Hartman: Good afternoon. Chairman Rounds
6 Ranking Member Rosen, thank you for your unwavering support
7 and for the honor of representing U.S. Cyber Command today.

8 I'm here to discuss the evolving strategic landscape
9 and our approach as we look forward to 2026. CYBERCOM's
10 mission is straightforward: We defend the nation from cyber
11 threats, we protect the Department of Defense's Networks,
12 and we support the joint force. We are dedicated to
13 ensuring the department's mission advantage, and providing
14 options across the conflict continuum to the President, the
15 Secretary of Defense, and the American people.

16 Achieving our assigned objectives in the mission set
17 forth by the President of "Peace through strength", requires
18 a force equipped with a strong warrior ethos and the
19 lethality necessary to meet our national objectives.

20 Deterrence is essential to our strategy. In
21 cyberspace, we're focused on maintaining a credible
22 capability that dissuades adversaries from targeting our
23 critical infrastructure. Cyberspace is a rapidly evolving
24 domain influenced by technological advancements, which
25 necessitates a close partnership with industry. As the

1 environment changes, CYBERCOM will adapt by swiftly
2 developing and deploying new capabilities. Our commitment
3 is to lead from the front, staying ahead of threats, through
4 a proactive and agile approach.

5 Our people are our greatest asset, capturing our ethos,
6 we win with people. The dedicated professionals of CYBERCOM
7 are at the forefront, defending networks, encountering
8 threats every day. Their innovation and perseverance are
9 essential to maintaining our nation's advantage in
10 cyberspace.

11 But we're not alone in the fight. Our allies and
12 partners are crucial components of our collective defense.
13 Key collaborations like our partnership with the National
14 Security Agency, enhance our nation's security by creating a
15 unified effort that surpasses the capabilities of our
16 adversaries.

17 Moving forward in 2026, our focus is not only on
18 maintaining readiness, but also elevating the level of
19 mastery within our cyber forces. Our initiative, CYBERCOM
20 2.0 seeks to overmatch our adversary's quantity with the
21 quality of our people, capabilities, and operations.
22 Modernizing our force design and rapidly integrating new
23 technologies, are vital components of our strategy here.
24 Partnership with industry and academia become indispensable,
25 enabling us to stay at the forefront of cybersecurity

1 advancements.

2 Our adversaries are persistent and they are
3 sophisticated. State sponsored cyber actors from China,
4 Iran, North Korea, and Russia, pose significant threats to
5 our critical infrastructure and military systems. China is
6 the most persistent threat while Russia has gained
7 significant capabilities through their ongoing operations.

8 To counter these threats, CYBERCOM develops robust
9 deterrent strategies, ensuring that any attempt to undermine
10 our security will face an overwhelming response. An
11 essential part of our future strategy includes the
12 accelerated integration of artificial intelligence.
13 Artificial intelligence offers unparalleled speed and
14 precision in cyberspace operations, making it a key enabler
15 for anticipating and countering emerging threats.

16 By expanding AI across our operations, we will
17 strengthen our deterrence posture and maintain superiority
18 in the cyber domain. True excellence in AI requires a world
19 class workforce. Through initiatives like CYBERCOM 2.0,
20 CYBERCOM will continue to collaborate with the department to
21 develop, pilot, and implement new tools and opportunities to
22 invest in our workforce. A world class workforce requires
23 world class training, facilities, and capabilities to excel
24 and thrive. With the support and assistance, we received
25 from the department and from Congress, CYBERCOM is well

1 positioned to achieve these world class results.

2 Our work is far from finished, but with your continued
3 partnership, I'm confident we'll succeed in defending our
4 nation. CYBERCOM is prepared to rise to the challenge,
5 outpacing our adversaries, securing our interests, and
6 protecting our future.

7 Thank you, and I look forward to answering any
8 questions you may have.

9 [The prepared statement of General Hartman follows:]

10 [COMMITTEE INSERT]

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 Senator Rounds: Thank you, General Hartman. I'll
2 begin. In the wake of the various persistent cyber threats
3 originating from the People's Republic of China over the
4 last two years, it is my firm conclusion that the importance
5 of the dual hat is as important today as it has ever been.

6 Given these events, how has the dual hat arrangement
7 between USCYBERCOM and NSA evolved to address the emerging
8 threats from our adversaries?

9 General Hartman: Senator, thank you for your question.
10 The relationship between CYBERCOM and NSA continues to
11 evolve so that we really achieve two key objectives. The
12 first is that we see and understand what our adversary is
13 doing. The second piece of that is that, we enable CYBERCOM
14 or other elements of the U.S. government in order to
15 operate, in order to defend our critical infrastructure, our
16 key networks and the Department of Defense Information
17 Network.

18 The ability for us to execute those operations clearly,
19 understanding that we have to act, but that we also have to
20 protect things like intelligent sources and methods, is
21 fundamentally important to the dual hat. From my standpoint
22 -- and Senator, I've been sitting on the campus of the
23 National Security Agency in CYBERCOM for most of the last 15
24 years, I've continued to see this partnership evolve, and
25 our ability to execute increasingly more precise operations

1 is fundamentally because the dual hat allows me, in my
2 current capacity, to move with the speed and agility of
3 unity of effort that is required, but it also forces leaders
4 across the organization to collaborate, to do the hard work
5 and to provide the best options for the national security of
6 the country.

7 That's what I believe is the importance of the dual
8 hat, and that is really where I believe we've evolved to.

9 Senator Rounds: Recognizing that this is an open
10 setting and we can't get into specifics. I think another
11 item, not only the dual hat, has been successful, but also
12 the NSPM 13, which was incorporated under President Trump in
13 his first term, I believe, has been very successful in the
14 process.

15 The determining of when you can do your offensive cyber
16 operations in an efficient manner, and making sure that all
17 parties involved are appropriately apprised, but there is a
18 decision process in place. Can you talk a little bit about
19 the successes in terms of just the magnitude of the
20 successes that you have seen achieved since the creation of
21 the National Security Policy Memorandum 13 by President
22 Trump in his first term?

23 General Hartman: Thank you, Senator Rounds for the
24 question. NSPM 13 is a repeatable, sustainable, agile
25 process that is recognized across the Department of Defense

1 and across the interagency that allows us to move at the
2 speed and agility that's required, based on our
3 intelligence, based on operational requirements, and it has
4 increased our ability to execute cyber operations tenfold.

5 Senator Rounds: Excellent. Thank you. This is just
6 to give the American public some sense of what happens when
7 you do the dual hat, and you also have the ability to make
8 the decisions and to move quickly, how quickly we can
9 actually accommodate our need for offensive cyber
10 operations. And thank you for that information.

11 Lieutenant General Hartman, in the commands testimony
12 last year, General Haugh previewed the CYBERCOM 2.0
13 initiative, to focus on delivering a bold step forward in
14 the future of the Cyber Mission Force. What is the status
15 of this effort and what are the major recommendations of
16 this plan?

17 General Hartman: Chairman Rounds, thanks for the
18 question. As you're well aware, one of the impetuses for
19 CYBERCOM 2.0 was Section 1533 of last year's National
20 Defense Authorization Act. Based on that, we put together a
21 planning team and really studied hundreds of different
22 references over the last year, and studied different force
23 presentation models. We briefed the recommendations of
24 CYBER COM 2.0 to the last administration and the Secretary
25 of Defense approved it. We briefed this to the new

1 Secretary of Defense who asked us to work the implementation
2 strategy that we were previously working on a six-month
3 timeline down to 45 days.

4 And so, we brought an operational planning team
5 together, or really what we called a cross-functional team.
6 And over the last 45 days, we've submitted a series of
7 recommendations that we have concurrence, generally from
8 across the services and across the department, which
9 honestly is pretty extraordinary in a 45-day time period,
10 for us to get that level of consensus.

11 Those recommendations are really built around how do we
12 improve talent management in the force? How do we improve
13 advanced training in the force? and how do we improve our
14 ability to innovate and bring new capabilities to the force
15 at the scale and speed that we need to compete with our
16 adversaries there.

17 That seems relatively simple. It's about 80 pages;
18 we've delivered it to the department. The department is
19 going through a very reasonable process and we're pending
20 the results of that feedback from the department Chairman.

21 Senator Rounds: Thank you General. Ranking Member
22 Rosen.

23 Senator Rosen: Well, thank you. I want to talk a
24 little bit maybe about policy challenges. So, as we
25 continue to evolve and develop our cyber capabilities to

1 address the emerging threats, it's clear that there's a
2 number of challenges, both within the Department of Defense
3 and across agencies that can impede everybody's progress.

4 And so, I'd like to ask you about these obstacles and
5 how they impact CYBERCOM's efforts to stay ahead of the
6 growing cyber threat landscape. And so, we know that you
7 have many challenges, but based on CYBERCOM's plan for
8 development, could you speak to some of the key policy
9 obstacles that remain challenges for your operations, both
10 within the Department of Defense and in the broader
11 interagency context?

12 General Hartman: Senator Rosen, thanks for the
13 question. First, I just want to highlight that I think we
14 have made significant progress. You know, one of the things
15 we have discussed previously is the ability for us to
16 support critical infrastructure that is off DoDIN, but
17 critical to the department's mission.

18 We do appreciate the support from Congress in giving us
19 the federal labs authority that has allowed us to execute
20 cooperative research agreements. I know that we've talked
21 about Guam being a key component of this, and, you know, I,
22 I'm happy to report that we have executed six different
23 craters over the last six months with a number of very
24 important critical infrastructure organizations in Guam.
25 And our assessment is we have reduced the threat that those

1 organizations face by about 25 percent.

2 And so that has been really key for us. We continue to
3 work to better integrate the reserve component into our
4 operations to help secure critical infrastructure. And it
5 is an area where we think we need both an improvement from a
6 policy standpoint, but we also need improvement from an
7 appropriation standpoint, so we're able to better leverage
8 the reserve component force in order to support some of
9 these critical mission sets.

10 Senator Rosen: So, could you elaborate a little
11 further maybe, with the primary sticking points what would
12 hinder that coordination effectiveness, expansion of our
13 cyber capabilities? And are you taking some steps there or
14 how can we help as we begin to think about what those policy
15 and appropriations needs might be?

16 General Hartman: Senator Rosen, thanks for the
17 question. I think on the defense of critical
18 infrastructure, there continues to be a key role that a
19 number of different organizations will take. And I don't
20 believe the department will necessarily be the lead, but you
21 know, there are recommendations that we will bring to the
22 committee to how we might better work with organizations
23 like the Department of Homeland Security, certainly
24 organizations like the National Guard Bureau and we do
25 believe that there are some policy recommendations that will

1 work through the process that will be beneficial.

2 I didn't talk about the United States Coast Guard. The
3 United States Coast Guard has been a key partnership over
4 the last 12 months. We have signed a memorandum of
5 understanding with the Coast Guard. And so, as a Coast
6 Guard executes operations under DHS authorities, we do have
7 the ability to support their operations, in a case where
8 they have an authority, but they don't have the capacity.
9 And certainly, as we look at the security of port
10 facilities, critical infrastructure that supports port
11 facilities, that is what we think is a very important MOU.

12 At the same time, if we have a CYBERCOM mission, we're
13 operating on a facility that is specifically suited to the
14 expertise the Coast Guard brings, they also have the ability
15 to reinforce our operations. And so, I do think we've made
16 progress. I think there are additional policy
17 recommendations. Senator, I look forward to working with
18 the committee in order to provide those recommendations.

19 Senator Rosen: Thank you. I want to talk a little bit
20 about cyber workforce, because you can't do any of this
21 without maintaining a robust cyber workforce. Our defense
22 posture depends on it, we have to be sure that they're
23 capable, that they're equipped, that they're trained, like
24 you're talking about, these are our challenges to constantly
25 be training, working on the mission, because the threats are

1 ever evolving. The cyber domain is incredibly dynamic and
2 achieving mastery it's just crucial, and it isn't done
3 overnight.

4 So what steps are you taking in CYBERCOM to make sure
5 that we're keeping our personnel ahead of the curve? And
6 talk to me about the workforce cuts and the hiring freeze
7 and how that's impacting your ability to meet the mission.

8 General Hartman: Senator Rosen, thanks. First of all,
9 I would like to highlight that over the last year, we've had
10 a number of things that have significantly impacted how
11 we're managing particularly our civilian workforce.

12 The first is the Cyber Excepted Service. The ability
13 to hire under CES has reduced the lag time by 45 percent,
14 from over a year to less than six months now, in order to
15 bring civilian personnel on board, that has been impactful.
16 We went through a transition from what we call a Combatant
17 Command Support Agency, from the Department of the Air Force
18 to the Department of the Army. I'm in the army, but I'm not
19 saying one is better than the other. But the transition,
20 you know, did provide a little bit of friction as we work
21 from one service to the other.

22 We transitioned to the army last June and that has
23 improved sort of a repeatable process to bring the civilians
24 on board. And then there have been things like the 4092
25 authorizations from Congress, that have been important and

1 allowed us to hire really, really high-end talent. So, I
2 think we are on a glide path.

3 The current hiring freeze has impacted our ability to
4 bring new hires into the force. And we'll continue to work
5 with the department on the way ahead for that. We have,
6 however, not been impacted by any cuts. We have been able
7 to go back to the department and get an exemption.

8 It is important because, as I think you're aware,
9 Senator, we're only a little over 50 percent man with our
10 civilian force but It's because those authorizations have
11 all come really in the last year and a half. So, we do
12 think it's important to get the civilian hiring freeze
13 moved, and we do think it's important to be able to rapidly
14 bring talent into the force.

15 Senator Rosen: Thank you.

16 Senator Rounds: General, I have just one other
17 question. In early 2024, Congress received a briefing on
18 the commands AI roadmap as required by the fiscal year 2023
19 National Defense Authorization Act. Given the release of
20 the Chinese generative AI model, DeepSeek-R1, what steps has
21 the command taken to accelerate delivery of the capabilities
22 and milestones in this roadmap? And what is needed to make
23 certain that we will be successful in this acceleration?

24 General Hartman: Chairman Rounds, thanks so much for
25 the question. And so over a year ago, we produced again,

1 based on a congressional requirement, so thanks, our AI
2 roadmap that laid out a plan for the next five years. Very
3 close partnership with NSA, and their artificial
4 intelligence experts. And a little over a year ago, we
5 decided that we had a really good plan from a staff
6 standpoint, but where CYBERCOM could add value, was in
7 operationalizing these capabilities.

8 So, we took the majority of the staff portion of that
9 AI task force, and we moved it to the Cyber National Mission
10 Force. We went out and hired some additional AI talent,
11 really focused on 90-day pilot projects that we could
12 evaluate, and if successful, we could scale across the
13 force. And if they weren't successful or didn't meet a need
14 that we would then focus our efforts elsewhere.

15 And so over the last 12 months, we have executed
16 artificial intelligence pilots to secure the DoDIN, right?
17 This is at the edge of the DoDIN network, this is across
18 network devices and it's at our end points. It has been
19 very successful, and it is where we're moving to in the
20 future.

21 We have integrated large language models into our "hunt
22 forward" kits. We have integrated large language models
23 into our offensive capabilities. We have partnered very
24 closely with DARPA, under Project Constellation and continue
25 to transition capabilities, mostly based on artificial

1 intelligence to the force.

2 Additionally, Senator, we have and will continue to
3 work with the department on long-term resourcing that
4 ensures we maintain advantage over China and any other
5 adversary. I will say, we were all -- paid close attention
6 to, and we're alarmed by the DeepSeek model, right, But the
7 United States of America builds the best software in the
8 world, all right. And we believe working with private
9 industry, working across the government, that unique
10 advantage in building the best software in the world, will
11 allow us to stay ahead of the Chinese.

12 Senator Rounds: Thank you General. Ranking Member
13 Rosen.

14 Senator Rosen: Thank you. I want to build a little
15 bit on Senator Round's AI question, because we look to the
16 future of cybersecurity. How else do we need, besides
17 artificial intelligence, how do we need to adapt our
18 training and development pipeline to ensure that our human
19 workforce achieves mastery in the cyber domain?

20 And additionally, with the increasing demands on our
21 personnel and the nature of the cyber operations, how else
22 can we perhaps leverage industry or commercial training
23 opportunities to supplement the more specific on-net
24 training that takes place in a classified environment?

25 General Hartman: Senator, thanks for the question.

1 You know, we've talked about CYBERCOM 2.0 and one of the big
2 ideas in CYBERCOM 2.0 is advanced training. right? And
3 right now, CYBERCOM is very fortunate and the services have
4 done a very good job in order to present a C2 force. And
5 so, the first time in the history of the command over the
6 last year, we've reached C2, which means manned 80 percent
7 in the aggregate and trained it to 70 percent.

8 But as we look at things like artificial intelligence,
9 and cloud computing, and data scientists, and other advanced
10 capabilities, we do think that the model we've laid out in
11 CYBERCOM 2.0 is really where we need to go. And it's my
12 role with service-like authorities and as a joint force
13 trainer, to take service members and civilians that are
14 presented to us by the services, and take them from that
15 basic level and make them masters. And that is masters in
16 data science, that's masters in cloud computing, that's
17 masters in artificial intelligence.

18 And then immediately take those lessons and feed them
19 back, not only into the training base from the services, but
20 also into our operational organization. That is really the
21 best way that we think we can get after the training part of
22 this. We are also working very closely with private
23 industry, the creator authority that the committee has given
24 us, also allows us to execute creators within private
25 industry. And we continue to work very closely with UARCs

1 and FFRDCs, who provide us access to really high-end, really
2 responsive talent, particularly as it relates to artificial
3 intelligence and machine learning.

4 Senator Rounds: Thank you. And I do believe we have
5 another member that is just arriving, and I would simply ask
6 Senator King, are you ready with questions?

7 Senator King: I'm always ready.

8 Senator Rosen: I was going to say I knew how he would
9 answer that. He's always ready.

10 Senator Rounds: Senator King.

11 Senator King: Thank you very much General for being
12 here today. I take it my colleagues have talked, I'm sorry.
13 I was at a hearing upstairs in the Intelligence Committee
14 and it was an open hearing, so I can even tell you about it.
15 But in any case, I understand that my colleagues have talked
16 a lot about the firing of General Haugh and how unfortunate
17 that was, so I don't need to plow that ground.

18 One of the issues that I'm principally concerned with
19 in cyber, is that we have no deterrent. Our strategy in all
20 of our other military and national security approaches is
21 based upon deterrence, except in cyber, where we continually
22 are attacked, as we were salt typhoon for example, going all
23 the way back to Sony, nothing ever happens to the adversary.
24 And my belief is, that until we start to impose costs and
25 they understand that there will be costs, these attacks are

1 going to continue, they're cheap, and there's really no
2 consequences.

3 If you're sitting in the Kremlin and somebody said,
4 let's interfere with the next election in the United States,
5 your answer would be, why not? It's not going to really
6 cost us anything, and they don't respond, we're not in at
7 any risk. Do you agree with me that we need to have a more
8 stronger retaliatory capacity, number one, and demonstrate
9 the will to use it? Otherwise, these attacks are simply
10 going to continue.

11 General Hartman: Senator, thanks for your question.
12 It's good to see you again.

13 Senator King: Yes, sir.

14 General Hartman: So, Senator, we certainly agree that
15 we need to continue to improve our capability in order to
16 deter and respond to attacks. I will tell you that from our
17 standpoint, there is certain activity that adversaries to
18 include China, will always continue to conduct. And we got
19 to focus on the most credible capabilities to deter
20 operations that significantly impact the national security.

21 Just like you, I am aware of salt typhoon and volt
22 typhoon, and while we're certainly concerned about that, and
23 we will certainly develop a broad range of options to deal
24 with that, I will tell you that the fact that we are able to
25 see and observe that activity, and we are able to work with

1 industry partners in order to build defenses against that
2 activity, is something that provides us some advantage vis-
3 a-vis adversaries like the Chinese.

4 And I assure you, we are dedicated to developing
5 options in order to counter that. And I would be more than
6 happy to work with your staff in a different setting to
7 provide you some details.

8 Senator King: Well, I understand that you have
9 capacity and you have capabilities. We demonstrated that in
10 2018 with the hunt forward, defend forward, that General
11 Nakasone initiated. So, I understand we have the capacity.
12 My problem is we don't have a doctrine. We don't have -- a
13 deterrence doesn't work unless the other side knows about
14 it. Dr. Strange love, why didn't you tell us about the
15 doomsday machine? Well, the Premier like surprises.

16 A deterrent isn't a deterrent: It takes two things,
17 three things, capacity-which we have, will-which we
18 apparently don't have and knowledge of the adversary that --
19 we have those two things, and that they're being held at
20 risk.

21 So, I'm not questioning the capabilities. What I'm
22 questioning is, here we are with salt typhoon, you know, two
23 or three, six months ago nothing's happened, no response,
24 no. You know, like I said, we haven't even responded to the
25 Sony attack, and that was 10 or 15 years ago. There's never

1 a price to be paid by our adversaries. And until we develop
2 that theory, it seems to the concept of deterrence, and let
3 them know that they're at risk, they're going to keep doing
4 what they're doing.

5 I understand defending and working with our private
6 sector partners, that's all good. But you can't patch your
7 way out of this. There's got to be, I believe, a credible
8 deterrent that the adversaries understand, that if they
9 attack us in cyberspace, they will pay a price. It doesn't
10 necessarily have to be in cyberspace. It may be some other
11 kind of harm that puts them at risk.

12 But the point is, until we start to develop that
13 doctrine and let our adversaries know, it's just going to
14 keep happening.

15 General Hartman: So, Senator, I acknowledge your
16 concern. Again, I look forward to working with the
17 committee, with the department and I do think we could
18 provide you some more information in a closed session.

19 Senator King: Well, I appreciate that. Thank you, Mr.
20 Chairman.

21 Senator Rounds: Thank you, Senator King. I do have
22 one last question for you, General and then I will allow
23 Ranking Member Rosen a final question as well.

24 Last year, the Defense Science Board briefed Congress
25 on the status of the Joint Cyber Warfighting Architecture or

1 JCWA. How is this command addressing the Defense Science
2 Board's concerns about excessive bureaucracy, and length the
3 acquisition timelines, that prevent cutting edge cyber
4 technologies from being integrated into the Joint Cyber
5 Warfighting Architecture, before they become obsolete?

6 General Hartman: Chairman Rounds, thanks for your
7 question. In the 2022 National Defense Authorization Act,
8 CYBERCOM was given a number of things, we put it under the
9 banner of service like authorities. One of those was
10 acquisition authorities. The other piece was enhanced
11 budget control.

12 And under those authorities, we have consolidated our
13 efforts as it relates to JCWA, and we are fielding relevant,
14 agile, and not obsolete capabilities, that are positioning
15 us to execute our UCP mission to defend the nation, as well
16 as to support key geographic commanders like Admiral Paparo
17 and INDOPACOM.

18 And we have a plan to take the six programs that are
19 part of JCWA, that have currently been developed by the
20 services, and to bring those underneath our program
21 executive office, really focused on offensive, defensive and
22 enterprise level operations. And it's working senator and I
23 look forward to providing you and the committee additional
24 updates on that.

25 Senator Rounds: Excellent. Senator Rosen.

1 Senator Rosen: Thank you. I actually have a compound
2 last question. So, I want a clarification on some terms
3 that we use on about the PRC. So, could you explain for the
4 layman what "living off the land" tactics are and why it's
5 important from a cyber defense perspective? And the
6 compound part of the question is, and finally, what do you
7 really want us to know that we haven't asked you today. We
8 know you've had just a short time to prepare for this, but
9 maybe we'll give you that final word there too.

10 General Hartman: Hey, thanks, Senator Rosen. So,
11 living off the land, you know, really describes when an
12 adversary gains access to your network and then uses
13 legitimate user credentials and legitimate user behavior in
14 order to live in your network, in a way that makes it really
15 hard to detect them using a standard antivirus or alert-
16 based program.

17 Senator Rosen: So secretly living in the basement, I
18 suppose then, right?

19 [Laughter.]

20 General Hartman: And so, it just, it makes it really
21 difficult because it's the behavior that you've got to
22 detect. But look, we do know how to do that. We have
23 gained a significant amount of knowledge. Artificial
24 intelligence is going to help us, working with private
25 industry is going to help us. And we're dedicated to

1 continue to get after that problem.

2 Senator Rounds: Thank you. And then I think Senator
3 King had one more question?

4 General Hartman: I didn't answer the second part of her
5 question.

6 Senator Rounds: Oh, I apologize. Go ahead.

7 General Hartman: And so, I think the thing that I
8 would most like the committee to take away is, Congress and
9 the department have given us authorities, right? They've
10 given us Service-like authorities. They've given us control
11 of the resources that apply to the - one, so the Cyber
12 Mission Force and the headquarters that employ them. We've
13 been given acquisition authorities, we've been given joint
14 force trainer authorities, and all those things are enabling
15 us to evolve the command in a way that better enables us to
16 compete with China or any other adversary. It is working.
17 Okay.

18 There are things that slow down the process: continuing
19 resolutions slow down the process, hiring freezes slow down
20 the process, transitions between one combatant command
21 support agency and the other, slow down the process. But we
22 have a plan, we're executing it, and it's all about the
23 ecosystem that we have to build that provides precise
24 intelligence to really smart capability developers, that
25 then field it to a force that has been trained and

1 operationally aligned to receive that capability.

2 We're doing it with DARPA, we're doing it with the S&T
3 community. We're doing it with the communities across our
4 services that have significant investments in cyber
5 capabilities. And we're doing it based on operational
6 requirements of geographic combatant commanders like INDO
7 PACOM, and based on CYBERCOM requirements to defend the
8 nation.

9 And so that's really the message I have here, those
10 authorities, those resources, they're relatively new, but
11 they are allowing us to really increase our ability to
12 really get after all the things that we've talked about
13 here.

14 Senator Rosen: Thank you.

15 Senator Rounds: Senator King.

16 Senator King: I realize this isn't exactly in your
17 lane, but it's certainly close. You talked in your prior
18 answer about the work with the private sector and alerting
19 them to the threats and to what was going on, and that's
20 very important. But the principal agency that actually has
21 performed that function as an interface between the federal
22 government and the private sector, is CISA.

23 And my concern is that we've seen reports of cuts at
24 CISA up to 90 percent. I believe 40 percent may be the
25 latest number. And I think they've eliminated the office

1 that interfaced with state election officials, that enabled
2 them to share threat data and information and protections
3 with state election officials to keep our election safe and
4 secure.

5 I am just puzzled, at a time of heightened cyber
6 threat, that we are essentially unilaterally disarming one
7 of the most important tools that we have to protect
8 ourselves in cyberspace. Do you have any views on the
9 dismantling of CISA?

10 General Hartman: Senator King, thanks for the
11 question. To be honest, I do not understand what the actual
12 decisions are for any reduction or reorganization as it
13 relates to CISA. I will tell you that we continue to talk
14 to CISA leadership, and we continue to share information
15 with CISA leadership as it relates to threats that are
16 relevant to their mission for defenses in the United States.

17 Senator King: Well, Mr. Chairman, I realize that
18 again, this isn't his land, but this subcommittee's dealing
19 with the issue of cyber, and CISA is one of our most
20 important tools to deal with that and they've been very
21 effective. And having worked with some members of the
22 private sector that have worked with CISA, it took years to
23 build a trusting relationship between this government agency
24 and these companies, as well as the state election
25 officials.

1 I remember when that initiative first started, and
2 those state election officials were very reluctant to
3 interface with this Federal Agency. But they became very --
4 I wouldn't say dependent, but they became very engaged with
5 CISA in the last several elections and to basically
6 dismantle that capability, I think is very dangerous for
7 national security at a time of heightened cyber-attack.
8 We're under attack right now, and to be unilaterally
9 disarming and disabling what amounts to a carrier fleet, I
10 think is very damaging to the security of the country.
11 Thank you.

12 Senator Rounds: I think Your concern is noted,
13 Senator. With that, I want to thank General Hartman for
14 coming in on short notice and participating in this
15 subcommittee hearing. This does conclude the open portion
16 of today's cybersecurity subcommittee hearing.

17 I'd like to once again, thank our witness, Lieutenant
18 General Hartman, for his testimony. For the information of
19 members, questions for the record will be due to the
20 committee within two business days of the conclusion of the
21 hearing. And with that, Senator, any final remarks?

22 Senator Rosen: No. Thank you for coming.

23 Senator Rounds: And with that, then this subcommittee
24 hearing is adjourned.

25 General Hartman: Thank you, Chairman, Ranking Member.

[Whereupon, at 4:27 p.m., the hearing was adjourned.]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25