Joint Service Academy Cybersecurity Summit April 4-5, 2023

Executive Summary

ARMY CYBER INSTITUTE AT WEST POINT

WEST POINT PRESS

Key Summit Speakers

- Gen. Paul M. Nakasone
- Rep. Mark Greene, M.D.
- Lt. Gen. Maria B. Barrett
- Vice Adm. Craig A. Clapperton
- Lt. Gen. Robert Skinner
- Maj. Gen. William J. Hartman
- Maj. Gen. Joseph Matos
- Rear Adm. John C. Vann
- Mr. Chris DeRusha
- Ms. Mieke Eoyang
- Mr. Rich Baich
- Mr. Colin Ahearn
- Maj. Gen. Matthew D. Dinmore
- Ms. Wanda T. Jones-Heath
- Mr. Christopher Cleary
- Dr. Michael Sulmeyer
- Rear Adm. Jeffrey S. Scheidt
- Mr. Mike Wagner
- Ms. Jen Buckner
- Mr. Barry Hensley
- Mr. Peter Kim

History

Created in 2015 by the ACI and its partner Palo Alto Networks, the Joint Service Academy Cyber Security Summit (JSACS) is an event series designed to rotate every two years amongst the three service academies. The two previous event iterations were hosted online by USAFA. West Point last hosted the event in April 2016 and has been a key contributor throughout the event's history. JSACS is attended by senior executives from the commercial sector who are service academy graduates and cyber leaders from the government, including the Department of Defense (DoD). The conference incorporates all service academies and their graduates. This conference attempts to better integrate the commercial sector with DoD cyber operations and Academy cyber education.

2023 Summit

Over the course of two half-days, key leaders from government, DoD, and industry gathered in Eisenhower Hall at West Point, NY, to discuss current topics in the cyber domain. Sponsored by Palo Alto Networks and supported by the Army Cyber Institute (ACI), this event provided a venue for cyber thought leaders to share their ideas and strategies with a broad audience, including cadets from three service academies. This document provides an executive summary of the discussions held during the summit. For those interested in the full discussions, videos of the panels and keynotes can be accessed at https://jsacyber.com.

Day One Sessions (4 April 2023)

Keynote - Gen. Paul M. Nakasone “A Call for Leadership in the Cyber

During his Keynote address, Gen. Nakasone highlighted the evolving challenges our nation has faced since 2019 and the last JASC summit. Among those, he framed cybersecurity within the context of national security. He also highlighted the rise of ransomware, the dynamic nature of the great power competition, and the "series of borderless challenges," including COVID-19, migration, climate change, and cyber. All of those things are further complicated by the changing scope, scale, and sophistication of our adversaries, as evidenced by the ascendency of Twitter trolls, the information-framing potential of platforms like TikTok, and the impact of disruptive technologies like ChatGPT. USCYBERCOM continues to meet these challenges by working to maintain a decisive and enduring technological advantage over our adversaries. By working with and through our strategic partners, USCYBERCOM contributes integrated deterrence, as put forth in the 2022 National Defense Strategy. We must "move fast with a purpose." Of all those things, one thing remains unwavering: USCYBERCOM is committed to recruiting, developing, and retaining talented people. This fight needs critical thinkers who are proud to be part of a professional cadre of problem solvers who can develop options and make recommendations. To quote Gen. Nakasone, 'We Win with People!

Panel - Cybersecurity Resilience: A Shared Congressional Priority

Bruce Byrd, Executive Vice President and General Counsel for Palo Alto Networks, talked with Chairman Mark Green, M.D., U.S. Representative from Tennessee’s 7th congressional district; Chairman, House Committee on Homeland Security about the state of Congressional support for cybersecurity. Chairman Green discussed how cybersecurity is a bipartisan concern, and as a result, there are already many accomplishments, including first-to-market incentives, the creation of a Department of State Ambassador for Cybersecurity, and improvements in technology acquisitions. He has sponsored a bill to better secure open-source data/information and acknowledged that more work needs to be done to inform the public of cyber activity, the implementation of risk models, and increase communication and efforts between the multiple committees in Congress so that cybersecurity is addressed with the whole of government. He said Congress maintains oversight over CISA to ensure it is resourced, has appropriate authorities, and can grow capability, visibility, and workforce. He acknowledged that the pipeline for cyber talent is too small and is working within the government to make it larger through pay incentives and updating ways to maintain a clearance. Lastly, he talked about how AI can help cybersecurity and be a force multiplier but will cause economic and workforce changes.

Day One Sessions (4 April 2023)

Panel - Perspectives from Pentagon Cyber Leaders

Maj. Gen. John Davis (Ret) moderated a panel discussion with Christopher Cleary, Principal Cyber Advisor, Department of the Navy; Mieke Eoyang, Deputy Assistant Secretary of Defense for Cyber Policy; Wanda Jones-Heath, Principal Cyber Advisor, Department of the Air Force; Rear Adm. Jeffrey Scheidt, Senior Military Advisor for Cyber Policy to the Under Secretary of Defense for Policy and Deputy Principal Cyber Advisor to the Secretary of Defense; and Dr. Michael Sulmeyer, Principal Cyber Advisor, Department of the Army. This session allowed the audience to hear, compare, and contrast the differing perspectives, roles, and priorities of cyber leaders within the Pentagon and their respective organizations. The principal cyber advisors emphasized their advisory roles to "support," "champion," and "advocate" as needed the cyber-related issues and efforts within their service. The panel drew out the need to discuss cyber in warfighting and the power of partnerships with industry. In his closing comments, Mr. Cleary highlights that "industry is now in this with us" and "they are legitimate military targets."

Day One Sessions (4 April 2023)

Panel - Harnessing Industry Innovation to Strengthen Collective Defense

The panelists - Mike Wagner, Jen Buckner, and Pete Kim discussed with moderator Barry Hensley the challenges faced by the industry, such as the need for digital transformation in support of teleworking, high security turnover rates, and an increasing skills gap in cybersecurity. They shared their experiences from military backgrounds and discussed their strategies for hiring and retaining talent, focusing on culture, training, and leadership. The panelists emphasized the importance of building resilience in the face of cyber threats and collaborating with industry competitors to combat these threats.

During the Q&A session, the panelists shared their perspectives on addressing the challenges facing the industry. Jen Buckner emphasized the importance of building a diverse workforce with different backgrounds and experiences to address the skills gap in cybersecurity. Pete Kim discussed the need for resourcing agility, which refers to the ability to allocate and reallocate resources to respond rapidly to changing threats. Mike Wagner discussed the importance of tracking cyber hackers to identify and neutralize threats before they cause damage. They also discussed taking the fight to the enemy, which involves actively targeting and disrupting the operations of cyber attackers. Overall, the panelists highlighted the importance of resilience and collaboration in the face of evolving cyber threats and provided valuable insights into the innovative approaches that industry leaders are taking to strengthen collective defense.

Panel - Managing Cyber Risk at the Federal and State Levels

This panel consisted of Colin Ahern, Chief Cyber Officer, New York State; Chris DeRusha, Federal Chief Information Security Officer and Deputy National Cyber Director, Executive Office of the President and was moderated by Kelly Moan, Chief Information Security Officer, City of New York. The panel discussed how the National Cyber Security Strategy had provided a structure for a larger conversation across government and industry on the approach to cybersecurity. This includes providing guidance for how state agencies can advise their governors on risk, threat, resourcing, and policies; aligning and synchronizing regulations between state and federal levels; working across all state organizations; developing an education pipeline for cyber and information security expertise; providing value added to counties through training, brown bag lunches, and exercises; and creating business outcomes such as cyber resiliency, crime, misinformation, and ICS protection. These efforts will also provide feedback to the federal level to flush out further resourcing and policy requirements with a plan to revisit the National Cyber Strategy in three years to account for the rapid pace of technological change. The panel also discussed the unique roles and responsibilities that Federal and State actors can play in cyberspace using an "Operate, Collaborate, Regulate, Communicate" framework. This framework relies heavily on building trust and relationships at all levels and highlights the unique role of State and Local governments as direct service providers.

Day Two Sessions (5 April 2023)

Panel - A View from the Nation's Cyber Commanders

Members of this panel represented all of the military services, including the Reserve Component. The panel addressed the emerging trend of private actors maneuvering independently in cyberspace. This spurred a discussion by Maj. Gen. Hartman on the public-private partnership and the importance of information sharing to leverage each partner's relative strengths. This trend is captured in the National Cyber Strategy's concept of Integrated Deterrence, which Lt. Gen. Skinner acknowledged is the government's responsibility at the end of the day.

When discussing retention, multiple commanders said that one of the big draws of the military is the mission. There is an ability to do here what cannot be legally done anywhere else. The Coast Guard can expand on the available mission space. However, the fundamentals of warfighting and leadership are still key. Maj. Gen. Matos reinforced that no one is just part of Cyber; they're all part of the overall Joint Force. Vice Admiral Clapperton added the importance of connecting what your team is doing to the big picture. On leadership, Lt. Gen. Barrett mentioned that leaders need not underestimate their impact on their teams. They want to be led well. Maj. Gen. Dinmore, who conducts AI research in his civilian job, reinforced the importance of leadership by stating that he does not feel that there is going to be an AI that can be a leader at any time in the near future.

Finally, the notion of a distinct Cyber Service was posed to the panel. The consensus from the panel was that we are building capacity within our current formations, so without a deliberate scoping, defined problem, and holistic study, a Cyber Service is not needed now.

Day Two Sessions (5 April 2023)

Panel - Emerging Cyber Leaders

The JSAC Emerging Cyber Leader panel provided a counterbalance of perspectives to many senior leader panels during the Joint Service Academy Cybersecurity Summit. The panel, moderated by Dr. Edward Sobiesk, included 1Lt Allison Annick (USMC), LTJG Reagan Boccarossa (USN), Capt Nicholas Stryker (USAF), CPT Ryan Johnson, and CPT Kyler Kiriyama (USA). Each junior officer is currently a Cyber National Mission Force (CNMF) member.

Many ideas resonated throughout the conference, but the consensus among the panelists was the importance of human capital. 1Lt Annick encouraged senior leaders to obtain the best minds and more women in the cyber field. LTJG Boccarossa echoed the importance of talent from diverse backgrounds. As an Army representative, CPT Johnson elaborated on the importance of working with operators at the ground level to achieve easy wins when balancing mission speed and impact, while CPT Kiriyama emphasized the importance of collaboration with industry partners to deep dive into complex problems and enable cyber teams to focus on current operations. The mantra of "win with people" from Capt Stryker encapsulated the importance of people, collaboration, and talent management.

The panel provided perspective on topics previously not heard during the conference. Cyber leaders must learn to communicate with other communities, such as the infantry, to support the ground force commander. In addition, a few junior leaders emphasized how cyber operations are, and should remain, rank and service-agnostic, contrasting with normal military operations. These ideas showed how junior cyber leaders envision an improved and impactful future cyber force.

Day Two Sessions (5 April 2023)

Panel - A Fireside Chat on the National Cybersecurity Strategy

Wendi Whitmore, Senior Vice President, Unit 42, Palo Alto Networks, conducted a fireside chat on the National Cybersecurity Strategy with Chris DeRusha, Federal Chief CISO and Deputy National Cyber Director. During this session, Mr. DeRusha talked about the need to rebalance risk ownership so that security becomes part of the original plan with longer-term investments and reinvigoration of world partnerships in cybersecurity. He expressed the need to make it more expensive for cybercriminals to attack than the cost of companies deterring cyberattacks. He also talked about how Russia-Ukraine has demonstrated the need for public-private partnerships. The conflict has demonstrated that private support (e.g., communications, satellite support, energy, gas, supply chain, water, industry, and any business with data on the net) and even individuals can now be targets. He highlighted the need for government to provide intelligence to help set the defense.

Army Cyber Institute

2101 New South Post Rd.
West Point, NY 10996

https://cyber.army.mil

WEST POINT
PRESS