

Day-Con XVIII

Dec. 20, 2024

Summit Notes

Evolution Revolution

Once again many of us found our way into a shared physical space to learn, work and play harder in Dayton. It was very gratifying to see so many returning delegates, friends and family. Of course, we also mixed up the “gene pool” by introducing some new neighbors. There were even a couple of surprise visitors and drop-ins (you know who you are). Of special note was a Hacksec OG who left Dayton to seek fame and fortune in the Cybers. It was great to have fr0g with us once again. It was truly a surprise and brought back a flood of memories from the days before DHS existed and you could get a vendor table at Defcon if DT liked your T-Shirt. (Did you know that Hack-Sec Klahn (HSK) was the first hacker group to print multi-color T-Shirts? ;)

This year’s theme and tagline went through several iterations; “Legal in both the cyber and physical domains” (very wordy indeed), “Finally Legal” (snappier but also confusing, especially for our international delegates), We settled on EVOLUTION and pivoted to EVOLUTION REVOLUTION the day of the summit! Hopefully the rationale is self-evident from the opening slides.

[Angus Blitter](#) [“Greetings Neighbors” & Deep Fake Justice League](#) - Angus introduced the concept of the [Deep Fake Justice League](#), a group focused on making the world safer by addressing deep fake issues and promoting awareness. Angus mentioned that the Deep Fake Justice League would be the focus of the Packetwars campaign for 2025-2026. He outlined plans for recruiting players and developing narratives around deep fake awareness and prevention. Angus shared details about the soft opening of the Deep Fake Justice League at Corn Con X, where participants engaged in a scenario involving AI and deep fake technology. He discussed the lessons learned and plans for future events.

Day-Con alumnus, [Jacob Torrey](#) was the first official speaker delegate with ["Phishing in the deep blue Azure"](#) -Jacob presented a story about developing and deploying adversary-in-the-middle phishing detection across Azure tenants, highlighting the challenges and successes of the project. He highlighted the project's goals and the technical challenges faced during implementation. Jacob explained the detection mechanism, which involved using a cloned website Canary Token to identify phishing attempts. He demonstrated how the system alerted users to potential threats before they entered their credentials. Jacob shared the outcomes of the project, including the detection of phishing attempts within the first day of domain

registration and the positive feedback received from users. He emphasized the importance of early detection in preventing successful phishing attacks.

[Matthias Luft](#) challenged the delegates with his radical thinking, entitled "[The Technology Optimist's View on Product Security](#)" - Matthias shared his perspective on cloud security, emphasizing the improvements in technology and the potential for optimism in the field.

"A fireside chat with [Tom Cross](#)" – Angus and Tom take a trip down memory lane as they reminisced and lamented over the systems of old and what the future of (anti)Social Media might look like. Tom discussed the evolution of social media, the challenges of content moderation, and the impact of business models on user experience. Tom shared the history and impact of his [Memestreams](#) project, highlighting its early adoption of social media algorithms and its influence on later platforms. Tom discussed the rise of new social media platforms, such as, [Mastodon](#) and [Bluesky](#), their potential for innovation, and the challenges they face in gaining user adoption. Tom discussed the importance of reputation systems in identifying trustworthy individuals and objective facts, emphasizing the need for protocols and webs of trust. Tom highlighted the difficulties of content moderation on platforms like Mastodon and the need for a sustainable business model to support the necessary work. Tom expressed optimism about the future of social media, emphasizing the importance of open platforms and the potential for users to reclaim their voices and create positive change.

[Jan Harrie](#) "[Traverse the Path](#)" - Jan introduced his session on extraction implementations, discussing common archive attacks and the importance of secure extraction libraries. Jan explained various archive attacks, such as exhaustive attacks, password reset attacks, and zip slip attacks, and provided recommendations for preventing them. Jan shared real-world examples of archive vulnerabilities found in source code, highlighting the importance of secure extraction implementations. Jan discussed the release of Google's safe archive library and the importance of verifying its security, while sharing his experience in recommending security improvements. Jan summarized his talk, emphasizing the importance of investigating problem areas, using best practice implementations, and learning from security research.

[Dr. Shawana Johnson](#) "[What Is Happening in Space – a Cyber Brief](#)" - Shawana discussed recent Chinese advancements in space maneuverability, including launching satellites from naval vessels and flipping large Earth observation satellites upside down. Shawana provided insights into the Chinese weather balloon incident, highlighting the importance of understanding space maneuverability and its implications. Shawana highlighted the growing investments in military cybersecurity, with a focus on protecting against adversarial attacks and enhancing capabilities. Shawana discussed her involvement in a book on space domain awareness and object identification, emphasizing the importance of identifying and analyzing space objects.

[Matthew Canham](#) "[Introduction to the Cognitive Security Institute](#)" - Matthew introduced the Cognitive Security Institute, explaining its focus on cognitive security and its intersection with social engineering, AI security, and disinformation. Matthew presented the Cognitive Attack Taxonomy, an open-source repository of cognitive vulnerabilities, exploits, and TTPs aimed at understanding and mitigating cognitive attacks. Matthew provided an overview of the Cognitive Security Institute's weekly meetings, covering a wide range of topics related to cognitive security, AI, and disinformation.

[Andy Prow](#) posited more radical thinking by challenging the status quo and the challenges of "[Keeping Humans Safe in a Modern Technological World](#)" Andy and team are collaborating with nations in Oceania to proactively write a digital safety roadmap for New Zealand and Australia. The delegates were all very excited by his call to action and agreed to support as appropriate.

Angus kicked off the final [session](#) by introducing the newest member of the Deep Fake Justice and [Packetwars](#) commentator [Glitch 2.0](#) . He also introduced the newest talk track ***The Glitch Index*** which fed the facilitated round table rant fest. His closing remarks promised Day-Con XIX would be 100% in person and once again re-invent learning, working and playing harder in Dayton.

Save the date for this years' 19th year September 13th, 2025 and keep an eye out on the socials for stories from the delegate reception and after party.