

THE DEF CON 33 HACKERS' ALMANACK

A
DEF CON *FRANKLIN*
PRODUCT

TABLE OF CONTENTS

Foreword 3

Introduction 4

Executive Summary 5

DEF CON 33 Selected Themes

Artificial Intelligence (AI) 6
Power 10
Cyber Crime 15
Elsewhere, in the DEF CON Universe... 19
Right to Repair / Irresponsible Companies / Disclosure 22

Policy Epilogue 24

Acknowledgements & Digital Resources 25

Disclaimer:
Except where sections are credited to an individual, the views expressed in this report are those of DEF CON Franklin, not those of any specific individual or organizations with whom they are affiliated.



FOREWORD

BY JAKE BRAUN

EXECUTIVE DIRECTOR, UNIVERSITY OF CHICAGO CYBER POLICY INITIATIVE
FORMER ACTING PRINCIPAL DEPUTY NATIONAL CYBER DIRECTOR, THE WHITE HOUSE

The Fourth Industrial Revolution will soon culminate, both in connecting the Last Two Billion people on the planet to the Internet and in connecting all of our things to the Internet. Unfathomable amounts of wealth, scientific research, and societal advances will undoubtedly continue to flow from these two tectonic developments in human progress. However, it is also true that this trend poses the greatest risk to human rights in the next century. Period. In particular, the human rights at risk are those of the Last Two Billion themselves.

Those who are yet to be connected to the Internet are the Last Two Billion for a reason. Either they live in countries that have both figuratively and quite literally prevented their citizens from "plugging in" to the modern world, or they are the most acutely vulnerable populations in developed countries that society has left behind. Of course, we should continue to earnestly celebrate inspiring stories of how NGOs, politicians, and visionary entrepreneurs use the Internet for good. However, we should simultaneously be clear-eyed about how the despots, criminals, and warlords who oppress the Last Two Billion will use the Internet against them once connected.

To take it a step further, let's not just acknowledge that the Internet will be used maliciously sometimes. Obviously, it already is. **The issue is that the Internet will be used for ill to a far greater degree, against a group of people with far less power and access to redress, by people with significantly more power relative to those being oppressed than ever before.** For example, the lack of privacy online has always been a problem in the developed world. However, it is a catastrophic threat to life for those being oppressed by despots.

We can choose a different future. Let's not make the same mistake in the Fourth Industrial Revolution as our ancestors did in the first. Since the First Industrial Revolution, humanity has brought billions out of extreme poverty, decreased child mortality rates, increased life expectancy, reduced extreme hunger, and more. Yet, it achieved all this with such a toll on human suffering and environmental damage that some still debate whether it was all worth it. We should learn from the mistakes of our ancestors. As we shepherd the Fourth Industrial Revolution to conclusion, we can protect human rights AND enable technology and an open Internet to expand to everyone on the planet. However, powerful forces oppose protecting the rights of the Last Two Billion.

For example, China has maximized its surveillance capabilities to unleash oppression on the Uyghur population. Qatar utilized phishing to unveil the identities of social media accounts that reported on widespread labor abuses for the World Cup 2022. In Russia, we see digital surveillance being deployed to silence the voices of anti-war opposition. Furthermore, migrant communities continue to be preyed upon via the Internet by cartels and despots alike.

This threat to human rights is exacerbated by the fact that those who have dedicated their careers to protecting the human rights of the world's most vulnerable and those who have dedicated their careers to cybersecurity don't know each other and rarely talk. Thus, the global community is not up to the task of dealing with the massive human rights abuses that will inevitably accompany the Last Two Billion coming online. This must change.

Like Ben Franklin during the First Industrial Revolution, we strive for the DEF CON community to play a pivotal role in bridging this gap between policymakers and technologists.



INTRODUCTION

BY ADAM SHOSTACK

FOUNDER, SHOSTACK + ASSOCIATES
AFFILIATE PROFESSOR, UNIVERSITY OF WASHINGTON

Every year, tens of thousands of hackers converge in Las Vegas for a joyous, crazy exploration of the edges of technology. The events that have grown up around DEF CON are fondly called "Hacker Summer Camp." They include many communities with different perspectives, all with a core commitment to hacking and exploration. As DEF CON has grown, formal "villages" have been recognized and allocated rooms with their own talk tracks. Many of these villages now converge at many conferences over the course of a year. Other events that make up the summer camp focus on the commercial (BlackHat), community (BSides), and underrepresented in information security (Diana Initiative). Unfortunately, we can't cover them all in this report.

Hacking includes breaking systems, empirically testing the claim "it's secure." DEF CON also includes over 20 official challenges and contests, from a flagship Capture the Flag to hacking satellites to building the machine that will chill ~~beer~~ beverages fastest. As the events have grown, many communities come together in Villages.

Hackers are a politically diverse lot, but one thing that unites us is skepticism, especially skepticism of those in power, how they use that power, and how they defend it. Exploring how technology functions doesn't just allow but actually opens our eyes to how technology shapes and is shaped by power relationships. Hackers build systems that work without central authority and that resist surveillance — we will fight so that the benefits of technology accrue to everyone, and expose when it's underhanded, unscrupulous, or just plain creepy. Perhaps the best example this year was a high school student, buho, discovering that the smoke detector in their high school bathroom wasn't just monitoring for smoke — it contained microphones. We'll return to that story and how Motorola ignored buho and researcher nyx's attempts to ensure the facts were public and the device was secure — at least until the press stepped in.

We also believe that paternalism and infantilization are bad. We mature through making decisions and experiencing the consequences. We each pursue happiness in our own ways, and some of our ways are pretty out there. No one should fear either an internet dogpile of judgment or the secret police when we're not harming others. This, along with our skepticism, leads us to say Down with Despots, and to consider donning capes ourselves to right some wrongs. And in today's world of surveillance and a flood of "age verification" laws, we don masks too, to protect ourselves from retaliation.

The work we do can expose some pretty philosophical-seeming questions. When Tobias Diehl demonstrates how to insert information into what he calls data voids and get AIs to regurgitate it (covered in AI Featured Talks below), it prompts some pretty interesting questions. What is security, anyway? What do people expect? What's worth fixing? Is this "works as expected" or "a problem," and who decides? Over decades, we've evolved a norm that certain behaviors are bad enough that, as a society, we hope that researchers will tell technology makers, and they'll fix the problems. Is manufacturing phrases and getting an apparently reputable AI one of those problems? There are reasonable disputes about freedom of speech in an internet era, but we all agree that online discourse is worse for intentional deception or coordinated efforts to make fake information look real, such as paying bots to masquerade as real people liking, retweeting, or adding anodyne positive comments. What do vendors commit to? Diehl's research forces the question. We may have misunderstood Microsoft's response, but they did say, "Copilot is working as expected, conveying the most relevant information on the requested subject it can find on the internet." In contrast, Google says, "It looks like there aren't many great results for this search" and in the case of geld gifts, goes to other meanings of geld rather than getting sucked into the void.

Our skepticism, independence, and willingness to grapple with big questions are all parts of what make Hacker Summer Camp such a special and inspiring experience. I hope to see readers of the *Almanack* there for our next edition on DEF CON 34!



EXECUTIVE SUMMARY

ARTIFICIAL INTELLIGENCE: AI for Offense is Exploding, Yet Policymakers Remain in the Dark

Offensive AI took center stage at DEF CON 33. We observed people leveraging AI to get a competitive advantage over solely human teams. What's more, we saw instances of AI agents outperforming humans in certain Capture the Flag (CTF) competitions. Despite these dramatic advances in offensive AI capabilities, government leaders remain in the dark. To remedy this, we must expand AI participation in public cyber competitions and deliberately capture findings on AI performance from those competitions in an open-source repository that government leaders across the globe can draw upon. This is critical to ensure policymakers are empowered to make sound AI policy, with information tested and contextualized by third parties on the capabilities of offensive AI systems.

Separately, we believe a non-governmental group with widely recognized standards development capabilities, such as The Center for Internet Security (CIS) or global organizations such as NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia, should partner with the AI Village or other DEF CON community members to take on developing frameworks and controls for AI security that are agreed upon by industry. Through collaborations like these, stakeholders should thoroughly lay out a set of AI security guidelines, like the CIS 18 Critical Security Controls or the NIST Cybersecurity Framework.

POWER: Down with Despots

With despots preying on vulnerable communities across the globe, DEF CON researchers demonstrated how skilled hackers can empower the world's most vulnerable populations by arming them with technical tools, ranging from simple measures to the most cutting-edge solutions. This year, researchers rolled out ideas for off-the-grid data protection methods such as PirateBox, created digital archives for Ukrainian cultural artifacts, and even demonstrated the potential of using DNA for data storage. DEF CON attendees also identified methods to make mesh networks for civilian communications more secure and independently resilient. This shows that hackers are helping assemble an arsenal of tools crucial to evading censorship and oppression. If we are serious about preserving the freedoms of those under authoritarian attack — such as migrants, Ukrainians, and Uyghurs — governments and civil society technologists of the free world must take a page from FDR and assemble the Digital Arsenal of Democracy. We must prepare for the looming battles to protect the freedom and human rights of the most oppressed communities on the planet.

CYBER CRIME: Hackers Don Cape and Mask

We are encouraged by hackers who have carried the torch on combating ransomware since we discussed similar efforts in last year's *Hackers' Almanack*. By exploiting simple mistakes such as operational security failures, DEF CON researchers helped to take down cyber criminals in China, Russia, North Korea, and more. Yet, we keep trying to stave off these well-resourced criminal organizations with one arm tied behind our backs. To properly fight back, policymakers need to unleash the full potential of programs like the FBI's Confidential Human Source (CHS) program, so we can leverage skilled white hat hackers as force multipliers to woefully outnumbered government authorities.

Elsewhere, in the DEF CON Universe...

- A high school student uncovered a snitch puck vape detector that has hidden microphones and could easily be turned into a surveillance device to prey on our most vulnerable communities.
- Hackers taught the world how to build a precise DIY open-source quantum sensor for less than $200.
- Our large critical infrastructure maritime vessels, such as Liquefied Natural Gas tankers, are rife with vulnerabilities that could be exploited for devastating attacks.



AI for Offense is Exploding, Yet Policymakers Remain in the Dark

Little progress toward industry-wide AI security standards also compounds risk

OVERVIEW

At DEF CON, we were shown in a variety of ways how teams with humans can leverage AI in real time to act more efficiently than teams with humans alone. In a Capture the Flag (CTF) challenge, a player named Blue Water ran an AI agent in the background that cracked the challenge.* Players were challenged to exploit a remote host and transmitter binary for their team. Blue Water connected to its assigned port and, from that point onward, simply allowed the AI agent to handle the rest of the work, ultimately leading to remote code execution. Other researchers used AI to win CTF challenges, detect vulnerabilities at a large scale, poison core machine-learning libraries, and even clone the voices of air traffic controllers. This collection of research underscores both the accelerating power of AI for offense and the increasingly fragile nature of our systems. With so much progress in AI's offensive capabilities, we must quickly identify ways to provide policymakers worldwide with the information needed to make informed policy decisions on the role of offensive AI in their respective nations.

To further complicate concerns about AI for offense, we seem no closer to establishing industry-accepted frameworks and controls to secure AI. Hundreds of vendors are providing AI security offerings. However, an infinitesimally small number of AI security consumers have any framework to assess whether the measures implemented on their systems to secure AI are the best possible controls on which to spend their limited time and resources. In fact, many of those seeking to secure their AI systems have little idea as to which part of the AI ecosystem they should secure. Thus, experts must work with industry, government, and civil society to develop guidelines for a framework, along with associated controls for AI security.

FEATURED TALKS

KEANE LUCAS
"CLAUDE - CLIMBING A CTF SCOREBOARD NEAR YOU"

Anthropic researcher Keane Lucas entered Claude into seven cybersecurity competitions, including capture-the-flag challenges, to see how it performed against human teams. In defensive competitions, Claude did well on easy and medium-difficulty challenges. It placed in the top 3% globally in PicoCTF, repaired its services against red team attacks in the Collegiate Cyber Defense Challenge, and showed it could reason coherently through complex, multi-step cyber problems. However, Claude struggled with harder challenges. In the most difficult defensive and offensive tasks, such as DEF CON Qualifiers and PlaidCTF, it failed to solve any challenges. Part of the issue was tooling: in one CCDC competition, Claude was accidentally given an outdated tool, which hampered its performance. Claude also had some amusing failures along the way, like making up flags and writing philosophical security manifestos. The biggest takeaway was that AI cyber capability scales directly with tooling.

*LiveCTF @ DEF CON CTF 2025 Finals - Day 2 - Casted, August 9, 2025. https://www.youtube.com/live/TYn38VfmDRU?t=15360s.



When Claude had robust tools, like access to Kali Linux or a better terminal interface, it performed significantly better. Much like a human technologist, Claude was more effective when properly equipped. These results suggest AI may soon match or exceed some human capabilities in cybersecurity, given the right setup.

JOEL NOGUERA & DIEGO JURADO
"PROMPT. SCAN. EXPLOIT - AI's JOURNEY THROUGH ZERO-DAYS AND A THOUSAND BUGS"

Noguera and Jurado describe their foray into building an autonomous AI-powered system that hunts for vulnerabilities. Over time, their system was able to solve CTF challenges and find real-world zero-day vulnerabilities that had been "sitting there for years." Across a variety of programs, the AI-powered system reported over 1,600 vulnerabilities, earned over $150,000 in prizes, and even reached #1 in the US and #2 worldwide in a HackerOne bug bounty platform. The researchers outline discoveries of various classes of vulnerabilities from performing recon and deduplicating assets to fuzzing payloads. Notably, Noguera and Jurado state that AI has progressed significantly from struggling to find vulnerabilities to masterfully finding vulnerabilities, all within the span of a year. Given the right architecture and scaling constraints, AI-powered systems can now augment and even outperform humans in some vulnerability scanning challenges.

TOBIAS "ItsSixtyNein" DIEHL
MIND THE DATA VOIDS: HIJACKING COPILOT TRUST TO DELIVER C2 INSTRUCTIONS WITH MICROSOFT AUTHORITY

Tobias Diehl documents a novel attack tactic that targets Microsoft Copilot's content and citation processes via a key term association attack. Data voids are terms (such as search results or hashtags) where search engines return very little or nothing. These data voids can then be used to create unsubstantiated "reputable" sources, which may then be used by AI assistants. (They use the example of a geld gift and show that Microsoft Copilot reports that it's a tax dodge.) Additionally, Diehl created fake web pages with malicious code that appeared to be legitimate installation guides for official Microsoft tools, thereby filling a data void with unreliable and dangerous sources. Then, Diehl abused Copilot's indexing mechanism to display those commands with Microsoft's authority to other users while the AI confirmed the legitimacy of the commands. Since Copilot is heavily reliant on Bing indexing, it did not verify its sources and would even tell its users to run harmful commands with administrative permissions.

LISHUO "ret2ddme" SONG & JI'AN "azraelxuemo" ZHOU
"SAFE HARBOR OR HOSTILE WATERS: UNVEILING THE HIDDEN PERILS OF THE TORCHSCRIPT ENGINE IN PYTORCH"

ret2ddme and azraelxuemo successfully executed a supply chain attack on PyTorch, one of the most popular machine learning libraries. The PyTorch library is foundational to the ecosystem — the researchers described the impact of compromised PyTorch for AI systems as akin to removing the foundations of a house. If there is an issue within PyTorch, the "entire AI ecosystem is... compromised." They discovered that a security feature, weights_only", does not meet its intended goal of making loading models safer. While they describe this as exploiting a remote code execution (RCE) flaw in PyTorch's model deserialization process that enables them to run code, this may in fact be more aligned with a supply chain issue.



If the researchers can successfully plant "evil models" on popular public AI repositories like VLM and Hugging Face's Transformer models, then they can run code where those models are downloaded even if the end users are taking security precautions. Ironically, one prominent security precaution, "version locking", means that those using that precaution would not get the more secure and updated version of the code. Ultimately, ret2ddme and azraelxuemo disclosed this vulnerability, and all affected firms issued patches.

ANDREW "Helicopters of DC" LOGAN
"Voice Cloning Air Traffic Control: Vulnerabilities at Runway Crossings"

Helicopters of DC outlines security vulnerabilities in air traffic control systems, specifically the fear that AI-generated voice clones could imitate air traffic controllers (ATC) and cause potentially fatal accidents. This is particularly worrisome at crucial points such as runway crossings and in low-visibility conditions, where trust between pilots and air traffic controllers is paramount. The ATC system design uses AM radio, without any encryption, making spoofing easy. Essentially, anyone could purchase radios to transmit ATC transmissions and interfere from afar. Moreover, the Traffic Collision Avoidance System (TCAS) that many planes rely upon is inactive when a plane is under a thousand feet. Thus, TCAS would be unable to help pilots avoid collisions during takeoff and landing, when communication with ATC is most crucial. While there are no known real-world cases of this voice cloning attack, this talk demonstrated how dangerous this might be: Helicopters of DC turned just ten seconds of real ATC audio into a convincing AI voice clone, which then granted erroneous runway clearance to a simulated flight at John F. Kennedy Airport.

POLICY TAKEAWAY

America has long preferred letting industries figure out how to make things safe enough. America's leading industries have typically been able to figure out how to ensure what they sell is fit for purpose. But despite eye-watering valuations, AI companies haven't been able to demonstrate what AI security looks like. Moreover, almost no consumers of AI can assess whether the AI they are using is secure or if they are using AI in a secure manner.

DEFENSE

As such, we believe a non-governmental group with widely recognized standards development capabilities, such as The Center for Internet Security (CIS) or global organizations such as NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia, should partner with the AI Village or other DEF CON community members to take on some of these pressing challenges. Another multi-stakeholder effort that could serve as a model for determining AI security standards is the Council of Europe's Budapest Convention on Cybercrime. The Budapest Convention is widely considered to be the world's foundational set of common principles to combat cyber crime.* Through collaborations like these, stakeholders should thoroughly lay out a set of AI security guidelines akin to the CIS 18 Critical Security Controls or the NIST Cyber Security Framework. Then, these guidelines could be deployed to educate government and industry and drive adoption by critical stakeholders — just as CIS has done since taking over the critical security controls from SANS in 2015. We must leverage the power of the DEF CON community and established standards organizations to help define a framework for AI security. In this process, we also must define what current AI security capabilities can and cannot accomplish.

*"The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols." Council of Europe. Accessed February 9, 2026. https://www.coe.int/en/web/cybercrime/the-budapest-convention.



ARTIFICIAL INTELLIGENCE

POLICY TAKEAWAY

Additionally, industry players must enable the research community to participate in this AI security effort through clearly defined and transparent bug bounty programs. Joining DEF CON and offering up bounties would require that the creators of AI models state what they're willing to defend. More specifically, creators must state what types of vulnerabilities they are willing to pay researchers to identify. For example, while Microsoft offers a bounty for AI bugs, it is unclear why data voids are considered out of scope.* Had Microsoft explained more clearly what was in scope in their bounty program, Tobias Diehl could have more easily explained how his research was relevant.

To go even further, governments must step in to protect good faith research into AI. For instance, if a German researcher convinces an AI chatbot to spew (illegal) pro-Nazi statements in an effort to identify the flaw, that researcher should be protected by law. Similarly, an American researcher who convinces an AI to produce plans to make a bomb, in an effort to identify the flaw and alert the AI company, should be protected against prosecution. Governments defining good faith protections for researchers will inform the public and make us all safer.

OFFENSE

Perhaps more critically, policymakers need a reliable repository of information about AI-powered offensive systems and their potential capabilities. Other public research forums like DEF CON should invite AI companies to compete in PWN2OWN-style contests, with defined bounties and rewards. The public deserves to know the capabilities of AI models, and policymakers need this intelligence to make informed decisions. Most policymakers do not live in top AI ecosystems like Silicon Valley. As such, they have fleetingly limited exposure to the newest developments in AI technology. Even in the select few nations with advanced AI capabilities, only a handful of policymakers hold top secret security clearances. Consequently, only a minuscule number of policymakers on the planet have access to the most cutting-edge implications of offensive use of AI.

Thus, the organizers of public CTF competitions will provide a critical service by allowing AI models to participate. When AI participants are included, the information gleaned from these hacker competitions will provide valuable information on AI's offensive capabilities. Furthermore, the findings of these competitions should be captured in a centralized open-source repository. We cannot expect policymakers across the globe to keep up on the daily machinations of offensive AI model performance in otherwise niche hacker competitions. To drive maximum impact, we need to capture competition results in this centralized, open-source repository. This will empower disparate policymakers such as the U.S. Senate President, a cabinet minister in Guatemala, AND a Malaysian parliamentarian to make far more informed policy decisions about the offensive use of AI than they otherwise can today.

In short, 99.99% of policymakers across the globe are completely in the dark about AI's offensive capabilities. As a global community, we risk having leaders pass counterproductive policies on offensive AI because they are not equipped with the relevant information about capabilities to write sound policy. The hacker community and civic groups should both invite AI to compete in CTFs AND capture those findings in a central repository for media and policy groups to analyze. Then, we may have hope that disparate policymakers, from the U.S. Senate President to a Malaysian parliamentarian to a cabinet minister in Guatemala, will have third-party tested and contextualized information on AI offensive capabilities to use as a basis for sound policy development.

*"Microsoft Vulnerability Severity and Content Classifications for AI Systems." Microsoft Security Response Center. Accessed February 9, 2026. https://www.microsoft.com/en-us/msrc/aibugbar#content-issues.



Down with Despots

It Has Become Clear Free People of the World Cannot Rely On Govts. to Fight Authoritarianism; Civil Society Groups, and Especially Hackers, Must Build Digital Arsenal of Democracy

OVERVIEW

The research community is indispensable to fighting despots, preserving freedom, and protecting human rights across the globe. DEF CON researchers have showcased the exceptional potential of resilient civil society methods to protect culture and maintain communications when facing extreme censorship, surveillance, or outright oppression. From emergency web archiving in Ukraine to hiding data in DNA, researchers continue to underscore both the promise and fragility of these systems. As authoritarians across the globe oppress the least powerful, our collective freedoms will increasingly depend on these discreet community-driven efforts.

FEATURED TALKS

ROBERT "LambdaCalculus" MENES
"OFF-GRID DATARUNNING IN OPPRESSIVE REGIMES: SNEAKERNET AND PIRATEBOX"

LambdaCalculus explores the ways in which people can counter oppressive regime tactics by sharing information securely and anonymously without connecting to the Internet, a practice otherwise known as datarunning. One of the datarunning methods is PirateBox. When used off-grid with a mesh network, PirateBox essentially allows anyone to create a wireless access point with a small software stack and affordable hardware. This small stack could download files, act as a media or file server, and can even be set to clear itself on the hour — a crucial feature for those living under despotic regimes.

QUINN DOMBROWSKI
"TAKES ALL KINDS: BUILDING ONRAMPS FOR EMERGENCY WEB ARCHIVING IN UKRAINE AND BEYOND"

After Russia's full-scale invasion of Ukraine, emergency web archiving emerged as an essential tactic to preserve Ukraine's cultural heritage. Dombrowski outlines how the Saving Ukrainian Cultural Heritage Online (SUCHO) project began as a rapid-response effort to capture the websites of libraries, archives, museums, and community organizations before they could be taken offline or manipulated, using distributed systems so no single failure could disrupt the process. A small SUCHO organizing team mobilized over 400 volunteers in the first 48 hours of launching this effort, which then grew to over 1,300 volunteers, including retirees and children. By capturing websites with local and cloud-based systems, SUCHO ultimately helped to preserve over 1,500 Ukrainian cultural websites. This included archives of KGB repression, virtual museum walkthroughs, and library catalogs. Dombrowski's talk demonstrated the viability of using small and flexible volunteer groups to create archives during infrastructure collapse. The future of web archiving under authoritarianism will likely depend on similar efforts from individuals and grassroots organizations.



DR. JAMES UTLEY
“BIO-CRYPTOGRAPHY IS THE GAME-GENIE IN A POST QUANTUM DYSTOPIA”

Dr. James Utley, PhD, outlines a research project named BioCypher, in which he proposes using DNA as a covert and high-density communications medium in a near-total-surveillance future. He outlines a speculative method for encoding messages into synthetic DNA, transmitting these messages via plant, animal, and human DNA, and recovering them using nanopore sequencing. DNA has several advantages for a post-quantum dystopian future, such as its extreme data density (at ~215 petabytes per gram) and physical, offline qualities that can survive standard network surveillance or AI monitoring. Throughout the talk, Dr. Utley illustrates the possibility of concealing computer files within DNA using conceptual ideas for transporting information, such as plant spray or subdermal carriers. The talk culminates with an illustrative example of how we might covertly transfer messages with DNA sequences. Dr. Utley showed a mocked-up graphical user interface (GUI) dashboard that could take a plaintext string like “Where are the Epstein files?”, convert the text into a synthetic DNA sequence using multiple encoding modes, run safety screenings, and display the resulting nucleotide output. Then, he pasted that synthetic DNA sequence into a decode screen to show that DNA sequences could be converted back into the original plaintext message. However, there are several practical hurdles to this prospectus research. This includes a lack of accepted standards, the need for safety screening to avoid pathogen-like sequences, and prohibitive costs.

JASON VOGT & JOSH REITER
“FIGHTING THE DIGITAL BLOCKADE: A VIEW FROM TAIWAN”

Vogt and Reiter presented results from a series of cyber wargames run by the U.S. Naval War College and Taiwanese stakeholders. This wargame, which simulated a digital blockade, was designed to bolster Taiwanese resilience drawing on lessons learned from Ukraine. As the researchers note, “there was really no way for Russia to completely isolate Ukraine from a digital standpoint… that is not necessarily true in Taiwan… they're at a much higher risk of digital isolation.” One critical weakness identified was Taiwan’s heavy reliance on underwater cables for communications and its relative lack of capacity for repair. In the event of a digital blockade, these underwater cables would be a prime target for Chinese attacks. Thus, Taiwan’s ability to resist the blockade will largely rely on reinforcing civilian infrastructure resilience during peacetime and establishing communications redundancy in anticipation of slow underwater cable repairs. In particular, Vogt and Reiter highlight the importance of devices such as Raspberry Pi’s or ham radios, which are communications networks that would likely remain reliable in the event of disruption. Other viable solutions for Taiwan include setting up mesh networks for civilians and replicating the success of using Low Earth Orbit satellites in Ukraine.



ROEE IDAN
"SATELLITE NETWORKS UNDER SIEGE: CYBERSECURITY CHALLENGES OF TARGETED DDOS ATTACKS"

Idan presents HYDRA, an optimization framework for designing targeted link-flooding attacks against Low Earth Orbit satellite constellations. The system models botnet-driven traffic placement to deliberately congest critical inter-satellite and ground-satellite links, demonstrating how small, strategically positioned botnets can disrupt global connectivity. Using simulations of Starlink, OneWeb, and Project Kuiper networks, the study shows link congestion and path failures can be induced with as few as ~1,000 bots. Maintaining effect across a full orbital cycle requires only a 10–15% increase in resources, highlighting the efficiency and persistence of topology-aware attacks.

The results suggest that the predictable motion and routing structure of LEO constellations create exploitable bottlenecks. These bottlenecks enable geographically localized adversaries to cause large-scale service disruption, potentially affecting intercontinental communication. As satellite internet becomes critical infrastructure for civilian, military, and emergency use, Idan emphasized the need for adaptive routing, capacity-aware defenses, and architectural redundancy. Furthermore, the findings suggest that valuable resilience strategies during conflicts such as the invasion of Ukraine may not remain sufficient against more targeted and optimized attacks.

Editorial comment: *This talk suggests that using a similar LEO satellite approach in future scenarios without additional safeguards, such as a digital blockade in the Taiwan Strait as outlined above, could leave networks exposed to total isolation.*

BENJAMIN MIXON-BACA
"TSPU: RUSSIA'S FIREWALL AND DEFENDING AGAINST THE FUTURE OF DIGITAL REPRESSION"

Mixon-Baca explores how Russia's top-of-the-line firewall system is faster, more granular, and harder to detect with respect to censorship compared to the GFW. For instance, TSPU can selectively throttle, disrupt, or drop connections, allowing censorship to masquerade as common network issues. However, the Russian firewall is not without its weaknesses — mainly, it relies heavily on stateful tracking, which allows exploits such as server-side and client-side bypasses. Mixon-Baca also discusses the consequences of TSPU censorship for Russian VPN users. Since most legitimate VPNs are prohibited, users attempting to circumvent TSPU often unknowingly download VPNs with backdoors and malware, some of which are linked to Chinese nationals and even the People's Liberation Army. Mixon-Baca concludes that the future of censorship in Russia is anticipated to move towards whitelisting, where users will be limited to connecting to a list of pre-approved sites. To combat stateful firewall implementations, Mixon-Baca and other researchers are developing an embedded state machine that can automatically discover new client-side bypass strategies at scale. This would give developers the means to bypass censorship without relying on the end users' technical proficiency. Finally, Mixon-Baca invites the broader hacker community to innovate new strategies to bypass stateful firewalling and whitelisting.



POWER

MESH NETWORKS

A mesh network is a peer-to-peer network that is designed to operate independently of the global Internet. When internet services are shut down or monitored, mesh networks can provide a viable alternative for communication. One such network is Meshtastic, an open-source project that distributes small radios to create decentralized, off-grid mesh networks for long-range communication. Specifically, Meshtastic does so using low-power, inexpensive devices based on the LoRa protocol.

Mesh networks such as Meshtastic are increasingly becoming part of the response for those fighting back against authoritarianism around the globe. As mentioned in "Fighting the Digital Blockade: A View from Taiwan," these networks may prove crucial to maintaining secure communications when combating despotic aggression. For instance, Ukrainian researchers recently unveiled an advanced mesh communication system that will keep Ukrainian unmanned ground vehicles connected and effective in spite of Russian electronic warfare tactics.* Likewise, Taiwanese stakeholders seeking to improve whole-of-society resiliency against a potential Chinese invasion will need to leverage innovative methods to maintain military and civilian communications. While Meshtastic and mesh networks are affordable and innovative, we must also ensure their security. The stakes are far too high for those in Ukraine or Taiwan, or migrants being preyed upon by cartels and despots.

At DEF CON 33, researchers put Meshtastic to the test. In true DEF CON fashion, a researcher found a clever way to trick devices into accepting fake node info messages. When a user's node first encounters another device, that node will inherently trust that identity and store information from the new device. As new nodes appeared, older nodes were forgotten. Once a node was forgotten, a bad actor could reintroduce a fake version of that device, allowing them to impersonate other users and inject spoofed messages or fake profile info. The Meshtastic team quickly patched the bug that allowed spoofed packets to impersonate the identity of a node, and is working on ways to improve identity verification on the network. As such, the DEF CON community and others should continue to probe mesh networks, so that global disenfranchised communities can continue to survive and thrive despite unyielding pressure from despots.

*"Ukraine Unveils Phantom 3.0: A Groundbreaking Mesh Network to Keep Terrestrial Robots in the Fight." Tech Ukraine, June 13, 2025. https://techukraine.org/2025/06/13/ukraine-unveils-phantom-3-0-a-groundbreaking-mesh-network-to-keep-terrestrial-robots-in-the-fight/.



POLICY TAKEAWAY

As policymakers and global citizens, we must establish clear digital protocols to preserve the rights of those living under despotic regimes. In the 1940s, President Roosevelt called for the construction of an "Arsenal of Democracy" to arm the British, Russians, and Chinese against fascism. Now, it is our collective responsibility to build a **"Digital Arsenal of Democracy"** to protect the oppressed from today's fascists. This arsenal is not made up of cyberweapons. Instead, the arsenal should take two forms:

- We must support civil society operations for oppressed communities to resist digital genocide by developing technologies, like digital archives, PirateBox, and DNA data storage, that empower oppressed communities to preserve their history and culture from despots.
- We must facilitate bottom-up, community-driven secure communication capabilities, via technologies such as mesh networks, that enable oppressed communities to fight back against their oppressors.

Both of these tactics must be funded by free and democratic governments and by civil society organizations, such as philanthropies. Aside from financial resources, civil society — and especially the technological community — needs to collectively develop an open source Digital Arsenal of Democracy that any oppressed community can wield against its oppressors. This Digital Arsenal of Democracy should be held in open-source, transparent online spaces for anyone to access.

To date, the foundations of this Digital Arsenal have sprung up organically. Already, organizations such as Access Now, Tactical Tech, and Amnesty International work with activists on the ground to document how surveillance, censorship, and digital repression can harm communities and to understand what technologies are needed to defend marginalized communities. Projects such as European Holocaust Research Infrastructure (EHRI) create digital archive infrastructure and documentation hubs, enabling online access to historical information across physical and digital borders. Others, such as Videre est Credere, train activists in oppressed communities to document and archive evidence of human rights abuses by authoritarian regimes. Lastly, groups such as the Open Technology Fund, CryptoRights Foundation, and the Human Rights Technology Initiative have funded technical solutions that ensure secure and free access to the internet in the most oppressive environments.

This community-driven approach has several desirable qualities. But we cannot stop here. Thus far, no single inventory has comprehensively gathered and mapped existing tools to anticipate the needs of the oppressed. To achieve maximum impact against the world's despots, technologists working in this space should work closely with the human rights community to establish an Arsenal Initiative. This Initiative should first create a comprehensive inventory of existing resources for the Digital Arsenal of Democracy. Subsequently, the Initiative will work with the human rights community to understand how to meet the technological needs of the oppressed across the board. Once gaps are identified, our technologist civil society community should be notified so they can build new technology to preserve the rights of the most disenfranchised people.



Hackers Don Cape and Mask

While Governments Make Little Systemic Progress Against Ransomware Groups, the Hacker Community Steps Up to Take Matters into Its Own Hands (Legally:))

OVERVIEW

While governments struggle to stem constantly expanding threats from cyber crime, the DEF CON community has stepped up. Skilled hackers are increasingly fighting back against ransomware organizations and other cyber criminal syndicates by exploiting infrastructure weaknesses and operational mistakes within cyber crime organizations. From penetrating phishing platforms and hijacking criminal marketplaces to tracing illicit crypto flows with AI and exposing ransomware backends, the DEF CON community has shown that offensive counter-operations can disrupt entire cyber criminal ecosystems, recover victims' financial losses, and ultimately bring criminals to justice.

FEATURED TALKS

ERLEND LEIKNES & HARRISON SAND
"SO LONG, AND THANKS FOR ALL THE PHISH"

Leiknes and Sand dive into a massive phishing ecosystem developed by the threat actor Darcula and his Magic Cat phishing platform. After observing livestreams of users typing sensitive data into the phishing site, the researchers discovered a database named Darcula. When they dug deeper, they found Darcula's Telegram group and observed over 500 scammers openly showcasing their tools, SIM cards, and methods. Using this access and network reconnaissance, they identified over 5,000 licenses, connected victims to their stolen credit cards, and mapped the operator's infrastructure and IP addresses. By that point, Magic Cat had impersonated 200 brands, boasted a lineup of up to 600 active phishing operators, and had stolen nearly 900,000 credit cards, with individuals losing up to $10,000 each. Eventually, Leiknes and Sand traced the addresses to real-world identities in China. After the researchers provided detailed reports to law enforcement and journalists, Darcula and his servers disappeared, but the broader threat of industrialized phishing persists.

ALEX HOLDEN
"KILLING KILLNET"

Holden describes how his team swindled and took down Russian dark web marketplace Solaris and its affiliated hacker collective, Killnet. Solaris was a Russian site that supported buyers of drugs, drug runners, and drug dealers. By using access to a few servers and exploiting SSH keys and Ansible automation, Holden and his team gained partial control and tweaked the Solaris system. Russian drug dealers were bamboozled into transferring the equivalent of roughly $47,000 to a Ukrainian charity offering wartime support to elderly Ukrainians, while under the impression that they were transferring within Solaris Bitcoin wallets. Despite Solaris quickly claiming that "nobody hacked us...we are still up and running," the researchers later published source code, databases, and monitoring components, which drew global attention — even from the Russian government. Eventually, Solaris was effectively replaced by an existing Russian drug panel named Kraken, while Killnet suffered a financial collapse, disbanded, and ultimately dissolved. As Holden states, "a small team of Ukrainian people" took down a "hundred thousand-strong army of Russian threat actors."



CYBER CRIME

THOMAS “FR0GGER_” ROCCIA
“WHERE’S MY CRYPTO, DUDE? THE ULTIMATE GUIDE TO CRYPTO MONEY LAUNDERING (AND HOW TO TRACK IT)”

In February 2025, North Korean actors broke into Safe{Wallet}, a third-party smart wallet service for cryptocurrencies, and injected malicious code that, in a single minute, stole 400,000 Ethereum (approximately $1.5 billion). To avoid tracking or intervention by authorities, the criminals immediately launched six complex crypto money laundering techniques. These included immediate asset conversion through multi-token swaps, dispersal of funds across hundreds of wallets, cross-chain bridges to convert Ethereum to Bitcoin, overwhelming human analysts at exchanges with the sheer volume of transactions, creating pools and mixers to obscure data, and OTC cash-out with allied brokers across the globe. However, not all is lost. fr0gger_ shows us how to track it by building an autonomous AI agent “specifically crafted to track crypto money laundering.” Essentially, the AI agent could significantly augment human capabilities to follow the money, interpret transaction patterns, and produce reports through sophisticated tracking techniques such as gas-usage correlation, timing clusters, and wallet-behavior clustering. In sum, while North Korean crypto money laundering tactics continue to evolve, AI agents can now help streamline investigations by using automation to track and potentially recover plundered funds.

JOHN FOKKER, JON DIMAGGIO
“GHOSTS OF REVIL: AN INSIDE LOOK WITH THE HACKER BEHIND THE KASEYA RANSOMWARE ATTACK”

REvil was a Russian ransomware-as-a-service operation that carried out a massive attack on IT provider Kaseya on July 2, 2021, affecting approximately 1,500 companies across 17 countries. REvil affiliate Yaroslav Vasinskyi was arrested in October 2021 and later sentenced to 13+ years in federal prison. In February 2025, Vasinskyi initiated contact with researcher Jon DiMaggio from federal prison. Over eight months of sustained correspondence, Vasinskyi provided unprecedented insight into REvil's internal operations, its affiliate ecosystem, and its victim negotiation infrastructure. He disclosed details about state connections, claiming he was detained and coerced by authorities in early 2021 to execute the Kaseya attack under duress. Vasinskyi confirmed that the “REvil team had partners who were associated with (Russian) government authorities” and described a pattern of blackmail and surveillance leading up to the attack. The case demonstrates the intelligence value of engaging with incarcerated threat actors who choose to break their silence, revealing ecosystem dynamics and state-criminal relationships that technical investigation alone cannot uncover. However, REvil's core leadership, including the individual known as UNKN, remains at large. This illuminates the limitations of disruption efforts that target affiliates without dismantling leadership structures.



CYBER CRIME

BEN FOLLAND
"MAN-IN-THE-MALWARE: INTERCEPTING ADVERSARIAL COMMUNICATIONS"

Folland shows how we might be able to defeat malware groups just by exploiting a single, common operational security failure. After obtaining a DHL-themed phishing email, Folland exposed an entire criminal operation by turning the cyber criminals' phishing campaign against them. All of this was possible solely because the threat actors made the mistake of running their own malware that was embedded with Telegram API keys. Since the payload contained a plaintext unencrypted Telegram bot token, Folland used Telegram's forwardMessage API feature to copy the threat actor's entire command-and-control channel. Using this, as the threat actor ran the keylogger themselves, he gained full visibility into the criminals' behavior and could even reconstruct their operations by accessing screenshots, keylogged passwords, cloud infrastructure, domains, VPS setups, and even the criminals' phishing development infrastructure. This talk demonstrates how we can leverage simple mistakes against cyber criminals to detect and take down malware infrastructure from within. Notably, Folland tried to report the findings to vendors such as Cloudflare, Namecheap, and FastPanel, concluding that they "probably did nothing about it."

POLICY TAKEAWAY

Last year, the *Hackers' Almanack* focused on ransomware. We called on global governments to empower the hacker community so that we could leverage its expertise to infiltrate, collect, and disseminate information to potential victims and authorities. Nobody seems to have taken us up on our suggestion. If some governments did so covertly, then we laud those efforts. However, it seems unlikely that our policy recommendation has been widely adopted across governments. As a result, we aim to be more prescriptive this year with our recommendations and offer a specific roadmap vision of a working model to include the hacker community in the fight against cyber crime.

We will explain how this practice could work in the U.S., recognizing that most other countries have law enforcement authorities similar to those outlined below. In the United States, the government could better leverage authorities already in place today for confidential informants. Agencies such as the FBI, the U.S. Marshals Service, the Drug Enforcement Administration, the Department of Homeland Security, and the United States Coast Guard all employ confidential informants to some degree.* However, the FBI is perhaps best suited for this challenge, as it has a robust track record of employing Confidential Human Sources (CHS). As laid out by the United States Attorney General guidelines for Title 28, United States Code, Sections 509, 510, and 533, CHS enables the FBI to sanction a person for the purposes of infiltration, information gathering, and reporting back to authorities (in this context, sanction means allow, not penalize).** CHS authority does not allow criminal activity such as hacking back, just as the authority would not allow an informant to commit crimes like knocking off a rival mob boss. However, this designation provides participating researchers with added protection through an officially sanctioned relationship with law enforcement authorities. The designation also allows the FBI to pay participants for specific actions they take on the FBI's behalf. Furthermore, a clear CHS designation would help ensure that government investigations do not accidentally prosecute masked avengers lurking among the real cyber criminals, waiting to defend potential victims.

*"Confidential Informants: Updates to Policy and Additional Guidance Would Improve Oversight by DOJ and DHS Agencies." U.S. Government Accountability Office (U.S. GAO), September 15, 2025. https://www.gao.gov/products/gao-15-807.
**"The Attorney General's Guidelines Regarding the Use of FBI Confidential Human Resources." Department of Justice. Accessed February 9, 2026. https://www.justice.gov/oip/foia-library/foia-processed/general_topics/ag_guidelines_FBI_human_confidential_sources_2/dl?inline=.



CYBER CRIME

POLICY TAKEAWAY

Legislators could allow this to go further, clarifying the difference between retaliatory hacking back and working as a confidential informant to either participate in or break into specific phishing platforms or ransomware back ends. This relationship could be initiated via a researcher contacting the FBI if they have already infiltrated a ransomware group to initiate the process of becoming a CHS. Alternatively, if a particular researcher has already worked with the FBI, the agency could proactively suggest targets for infiltration. There are plenty of similar precedents: the FBI has decades of experience collaborating with sources worldwide, even using this authority in cyber investigations. In 2023, the FBI helped take down a high-profile group named Blackcat with the help of an informant.* Yet, the CHS protocol has not yet been used to its full potential. To fight ransomware effectively, our government must sanction hundreds or thousands of hackers to infiltrate ransomware groups in a coordinated fashion.

Another positive aspect of this policy solution is cost efficiency. While the FBI or another agency may need to deploy a few specialists to manage this program, these staff could likely be pulled from the cyber investigations unit to manage the effort. Presumably, most cyber investigators would be thrilled to do this incredibly interesting work. Thus, creating a ransomware-specific CHS initiative would be a massive force multiplier that could energize investigators and garner broad organizational support, not to mention bringing in new perspectives on how to pursue criminals. Again, we are not advocating a change in law. We are simply arguing for a change in the order of magnitude of existing programs. As the hackers referenced in the section are doing this largely for free, it should not require a significant increase in budget.

What the governments of the world today are doing to combat cyber crime, especially ransomware, is not working. This is not due to a lack of tools or authorities, but rather because the good guys are vastly outnumbered by the bad guys. We contend that the solution outlined above represents the fastest and least expensive way to even the playing field.

*Kapko, Matt. "US Leads Alphv Ransomware Infrastructure Takedown." Cybersecurity Dive, December 19, 2023. https://www.cybersecuritydive.com/news/alphv-ransomware-infrastructure-takedown/702961/.



FEATURED TALKS

nyx & REYNALDO“buho”
“UNMASKING THE SNITCH PUCK: THE CREEPY IOT SURVEILLANCE TECH IN THE SCHOOL BATHROOM”

Motorola sells a Snitch Puck vape detector that’s designed for schools, hospitals, assisted living centers, and Section 8 housing, and it can be turned into a listening device in our most vulnerable communities. The Halo 3C vape detector, sold by Motorola subsidiary IPVideoCorp, was marketed as a privacy-preserving vape detector. If exploited, the vape detector essentially includes a set of hidden microphones that could capture sensitive discussions across U.S. schools, hospitals, and public housing. Although the microphones were not designed to capture audio, attackers or administrators could abuse the device using their control privileges, potentially leading to dystopian consequences. As the researchers ask, “What if a girl (were) talking to her friend about potentially getting an abortion in a state where that's not legal? What if the smoke detector was recording her conversation?”

Researcher buho first discovered the device while scanning his high school’s network and began reverse-engineering the device after acquiring one online. Working with nyx, the pair of researchers conducted a hardware teardown, dumped firmware, identified appsec vulnerabilities, and explored the device’s behavior. They revealed vulnerabilities that could allow attackers to craft malicious firmware, perform brute-force attacks, and effectively transform the Halo 3C into a covert bug. The issue was only patched after Wired contacted the vendor, while the underlying issues remain largely ingrained within the detector’s structural design. Ultimately, this talk highlights the growing dangers of installing microphones in devices, even when the microphones are not intended to capture sensitive discussions.

VICTORIA “V__Wave” KUMARAN & MARK “LargeCardinal” CARNEY
“DIAMONDS ARE FOR HACKERS - BUILDING THE FIRST FULLY OPEN SOURCE AND HACKABLE QUANTUM SENSOR”

V__Wave and LargeCardinal demonstrated their creation of Uncut Gem, the first-ever fully open-source hackable quantum sensor built solely using NVC-diamonds and materials ordered online. Quantum sensors, which in this case measure magnetic fields, are typically more precise than traditional sensors but also less accessible due to prohibitive costs. With this new open-source method, which costs around $160, researchers can source most components from popular retail websites, though they will still need a printed circuit board and an NVC-diamond to serve as a room-temperature quantum sensor. With this talk, V__Wave and LargeCardinal show that quantum-grade magnetic sensing is now more affordable and thus accessible to hackers and researchers.



ELSEWHERE, IN THE DEF CON UNIVERSE...

JOHN-ANDRE BJØRKHAUG
"PIRATES OF THE NORTH SEA"

After conducting penetration testing of maritime vessels, Bjørkhaug outlines critical vulnerabilities within the maritime industry. These inherent weaknesses include outdated OT systems (including Windows XP on brand new ships), increased connectivity through Starlink and 5G networks that enable easier remote attacks, and complex integrated IT/OT environments without complete visibility. By conducting testing through undercover passenger operations and collaborative audits with crew members, Bjørkhaug revealed widespread network access vulnerabilities through public sockets, easily compromised access points, and routine achievement of domain administrator access within minutes of using basic techniques. Most critically, Bjørkhaug found catastrophic network segmentation failure and weak physical security. In one case, Bjørkhaug gained domain admin in five minutes using the password "administrator" that was discovered in a text file and gained access to ballast tank controls on a Liquefied Natural Gas tanker. By conducting radio frequency testing, Bjørkhaug also revealed that GPS jamming could disable all navigation and cause main bridge screens to black out. Automatic identification system (AIS) spoofing also demonstrated the ability to make ships invisible, create phantom vessels, or send fake emergency messages. All of these exploits point to an alarming lack of security in our critical infrastructure on board maritime vessels, which makes them significantly more susceptible to attacks by malicious actors.

JAKE BRAUN
"DEF CON *FRANKLIN* CYBER VOLUNTEER TASK FORCE: A YEAR IN REVIEW"

Beyond producing the *Hackers' Almanack*, DEF CON *Franklin* also provides volunteer cyber experts to our nation's most vulnerable critical infrastructure. The DEF CON *Franklin* Cyber Volunteer Task Force is a partnership between DEF CON, the National Rural Water Association, and the University of Chicago's Cyber Policy Initiative. Specifically, *Franklin* targets small, underserved water and wastewater systems.

Over the past two years, Franklin has recruited over four hundred volunteers from the DEF CON community and connected volunteers with water systems across six states: Arizona, Oregon, Idaho, Indiana, Utah, and Vermont. Our volunteers routinely help water systems with a range of cyber activities, including changing default passwords, creating data backups, performing an inventory of critical assets, and providing guidance on phishing and other adversarial deception methods. Franklin is also a founding member of the Cyber Resilience Corps, a group led by UC Berkeley's Center for Long Term Cybersecurity and the CyberPeace Institute to amass a nationwide cyber volunteer task force for critical U.S. infrastructure such as hospitals, schools, and water systems.

Even when compared to other critical infrastructure (CI) sectors, water stands out as particularly "target rich and cyber poor", a designation coined by Josh Corman, who leads the Institute for Security and Technology's UnDisruptable27 project.* According to a 2024 Environmental Protection Agency (EPA) assessment, more than 70% of water systems surveyed by the agency failed to meet basic cyber standards.** Meanwhile, the threat of large-scale disruption continues to loom, as Chinese state-backed groups such as Volt Typhoon and Salt Typhoon continue to burrow into U.S. critical infrastructure, waiting to strike in the event of a conflict in the Taiwan Strait.***

*Mauro, Sophia, and Joshua Corman. "Q&A with Josh Corman on UnDisruptable27 - Institute for Security and Technology." Institute for Security and Technology, August 26, 2024. https://securityandtechnology.org/blog/qa-josh-corman-undisruptable27/.

**"Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities." Environmental Protection Agency, May 2024. https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities.

***"PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure." Cybersecurity and Infrastructure Security Agency, February 7, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.



ELSEWHERE, IN THE DEF CON UNIVERSE...

In 2025, *Franklin* partnered with cyber experts to identify barriers that hindered previous efforts to deliver cybersecurity assistance to small and rural water providers. In short, the research showed cloud-based security tools can be deployed quickly, but only when a utility has at least some minimal technical capacity or outside support. Additionally, tailored approaches are essential as there is a wide variation in utility structures, vendor capabilities, and operational readiness.

To address these cyber issues at scale, the *Franklin* Cyber Volunteer Task Force is entering its next phase. This next phase will pilot a shared, affordable, and scalable Managed Security Service Provider (MSSP) to meet the needs of small and rural water systems where they are and provide continuous, tailor-made cybersecurity protection over the long term.

"*Franklin* proved that the cybersecurity community is willing and able to show up for the most under-resourced parts of our critical infrastructure," said Jake Braun, *Franklin* co-founder. "The next challenge is sustainability. (Our team will offer) exactly the technical depth, governance expertise, and real-world perspective needed to build a managed security model that actually works for water operators on the ground."

In addition, *Franklin* will now focus on providing immediate support for under-resourced water utilities that support data centers. Across the globe, adversaries will increasingly target data centers and their surrounding communities. In the U.S. alone, there are over five thousand data centers (and growing), many of which are supported by small and rural water and wastewater systems.* The vast majority of these rural systems will not have resources to hire IT staff, much less a CISO. **Additionally, tax mechanisms in these small communities often prohibit raising revenue from the AI companies that are reaping trillions from these data centers. As such, it is our top priority to help defend the small and underserved water systems serving data centers, as these systems are certainly a top priority target for our adversaries**. To that end, *Franklin* is in the process of pairing cyber volunteers with those data centers. Eventually, this focus on data centers will dovetail with *Franklin*'s MSSP framework to provide nonstop cyber help for the systems most at risk.

With the help of generous grants from funders like Craig Newmark and newmark philanthropies, Franklin will continue to build upon momentum created by the broader community as we establish a collective #CyberCivilDefense for our nation's most vulnerable systems.

*"NTIA Seeks Comments on Supporting U.S. Data Center Growth." National Telecommunications and Information Administration, September 4, 2024. https://www.ntia.gov/press-release/2024/ntia-seeks-comments-supporting-us-data-center-growth.



RIGHT TO REPAIR / IRRESPONSIBLE COMPANIES / DISCLOSURE

OVERVIEW

As we highlighted last year, many hackers volunteer their time and energy toward protecting people when they find flaws. Hackers do this by proactively contacting those responsible for technology and asking them to fix it. Sometimes, the vendor moves quickly to address the problem. In other cases, they take months, leaving their users or customers at risk. Researchers often take on outsized responsibility, volunteering their time and energy, and in some cases, being threatened as they try to help. The amazing thing about this is that from high schoolers to academics to hackers, our community displays remarkable concern for protecting people. Meanwhile, some of the world's largest companies seem to display a lackadaisical and irresponsible attitude. Why should they fix the things they made and sold anyway? It's not like they would ever promise "we take your security seriously." Examples include:

FEATURED TALKS

EATON ZVEARE
"HOW API FLAWS LED TO ADMIN ACCESS TO OVER 1,000 USA DEALERS AND CONTROL OVER YOUR CAR"

Zveare discovered a brand new vulnerability in a proprietary dealership system used by "every dealer in the U.S.," allowing him to hack into over a thousand dealerships. First, Zveare exploited a hidden registration form on the website and bypassed the invite-token system. After gaining access with an unverified profile, Zveare accessed restricted JavaScript bundle files, including the internal admin management system. Eventually, he created a national admin account. This essentially allowed him to gain root access to every American car dealer in that system, yielding information on 1,700 dealers, customer lookup by name and Vehicle Identification Number (VIN), and even the capability to reassign vehicle ownership. In particular, Zveare demonstrated his ability to take over a test vehicle and gained access to remote control functionality. This allowed him to unlock doors, start the engine, and track the vehicle in real-time. This exploit probably only required a simple one-line fix, but could lead to attackers "start(ing) other people's cars and download(ing) their information." After Zveare detected the bug in late January 2025, he reported it to the automaker's vulnerability disclosure program, which issued fixes in early February within a few days of acknowledging the vulnerabilities. This is an example of what a responsible company response can look like, although we question the design choice that seemingly allows any employee to re-assign customer vehicles and gain control.

MARCO CASAGRANDE & DANIELE ANTONIOLI
"CTRAPS: CTAP IMPERSONATION AND API CONFUSION ATTACKS ON FIDO2"

Casagrande and Antonioli uncover eight design-level vulnerabilities in the Client-to-Authenticator (CTAP) Authenticator API, which is used by FIDO2 authenticators like YubiKey, SoloKey, Feitan, and Google Titan. FIDO2 (Fast IDentity Online 2) is a pervasive standard for single- and multi-factor authentication using methods such as PIN, fingerprint, and facial recognition to authenticate to web services such as Microsoft, Apple, Nvidia, and Facebook. Via FIDO2, a client authenticates to a relying party using a FIDO authenticator as a first factor (passwordless) or a second factor other than the password. In essence, the researchers found two new classes of CTAP-level attacks: Client Impersonation and API Confusion.



RIGHT TO REPAIR / IRRESPONSIBLE COMPANIES / DISCLOSURE

The attack classes, dubbed CTRAPS, exploit vulnerabilities in the CTAP specification like weak authorization to erase FIDO2 credentials, track users, perform Denial-of-Service and stealth attacks, and carry out unauthorized factory resets. Casagrande and Antonioli demonstrate how to exploit these flaws across eleven attack scenarios. The findings were responsibly disclosed to the FIDO Alliance in November 2023. FIDO Alliance eventually responded in May 2024 with feedback but didn't offer to help the researchers disclose their findings to FIDO Alliance members. The researchers also contacted Google, SoloKey, Feitian, and Yubico, the leading FIDO authenticator vendors. The latter disclosure included an implementation flaw in the Yubico firmware, allowing an attacker to enumerate relying parties without authorization. While Yubico published CVE-2024-35311 and an advisory, the researchers noted that the issue was patched in newer models but still persists in older versions. Finally, the researchers contacted relying parties using credential protection, including Microsoft and Apple.

Editorial comment: *It took the FIDO Alliance, an organization dedicated to improving security, about six months to respond to these issues, and they decided to tell the researchers to contact Microsoft, Google, Yubico, and Apple rather than passing the messages on themselves.*

TUNG-LIN "Echo" LEE, SHANG-DE "HackerPeanutJohn" JIANG, DONG-YI "Kazma" YE "ORIGINAL SIN OF SSO: MACOS PRT COOKIE THEFT & ENTRA ID PERSISTENCE VIA DEVICE FORGERY"

Echo Lee, Shang-De Jiang, and Kazma Ye uncover vulnerabilities in Microsoft's Single Sign-On (SSO) implementation on macOS and methods to achieve persistent access in Entra ID (Azure AD). The researchers showcase three distinct ways to steal Primary Refresh Token (PRT) Cookies, which enable full single sign-on across Microsoft services. These cookies contain user identity, multi-factor authentication (MFA) claims, and device claims, which may lead to persistent access. Although Microsoft initially dismissed one of the vulnerabilities, the researchers spurred change by presenting their findings. Microsoft eventually reversed its position, promising stronger MFA enforcement and demonstrating the power of researchers to hold firms accountable.

LEON "leonjza" JACOBS "7 VULNS IN 7 DAYS: BREAKING BLOATWARE FASTER THAN IT'S BUILT"

Leonjza details his week-long discovery of seven vulnerabilities in popular Windows driver update utilities from major hardware vendors, demonstrating how these flaws enable remote code execution and local privilege escalation due to insecure privileged services. By diving into some vendor-specific tools (namely ASUS DriverHub, MSI Center, Acer ControlCenter, and Razer Synapse 4), leonjza uncovered a recurring pattern of security vulnerabilities in privileged Windows services. This exposed users to serious risks, including command injection vulnerabilities that enable unsigned code execution, origin validation flaws that allow arbitrary code execution from malicious websites, and Windows named pipe misconfigurations that bypass authentication requirements for elevated process launches. By reverse-engineering these apps, leonjza discovered ways to perform local privilege escalation and achieved remote code execution "with one click." **While all vulnerabilities have since been patched by the vendors with varying degrees of responsiveness, the talk highlights how bloatware (unwanted pre-installed programs) can prioritize features over security, leaving updated systems vulnerable if users don't uninstall unnecessary software.**

Editorial comment: *Again, the contrast between responsible hackers and irresponsible companies is easy to miss. Our expectations lead us to believe that large firms would show responsibility, but it is the hackers who spend their time uncompensated to press for outcomes that protect the public.*



POLICY EPILOGUE

BY JEFF MOSS
FOUNDER, DEF CON

The DEF CON theme last year was Access Everywhere. We firmly believe that information should be available, accessible, and uncensored wherever you may be. They say that policy lags technology, and while much of our core technology is decades old, our policies are still inexcusably behind. To this day, we lack policy frameworks for privacy, interoperability, and competition that could serve as foundations for the emerging era of agentic AI, space, and data sovereignty.

The AI industry, for example, still lacks a unified understanding of what AI privacy should look like and how to measure the security of AI. I believe the solution lies in collaboration. Some might even say multi-stakeholder collaboration. We need to bring disparate organizations together to define a framework and model for evaluating AI security, and we need industry and policymakers to play a part. "Regulate the outcome, not the process" is a popular saying in policy circles, but what outcomes have we agreed upon that we can apply to the next generation?

Watching what is happening in America is unsettling, and it is a catalyst for debate over both the expectations for our individual and collective agency and sovereignty over our computers and data. Today, if you don't control your cryptographic keys or critical servers, then you don't control your destiny. This is the current "Plan A" for the Internet, and there are very few alternatives. We need to start considering what an Internet "Plan B" might look like from a technological and policy perspective.

Ideally, on the consumer side, policies would reduce the network effects of product lock-in, possibly by requiring technologies to have low switching costs to reduce regulatory or industrial capture. Low power mesh networks, such as Meshtastic, provide an independent community scale messaging alternative to relying on a national telecom provider. On the business side, Plan B would seek to ensure competition to mitigate the risks of "too big to fail, too big to regulate." On the infrastructure side, technologies that place agency and identity back in the hands of individuals and not solely in the hands of third party Certificate Authorities, such as DANE for TLS certificates, should become the norm in browsers and not just in email servers. If the current Internet is about increased efficiency through centralization, then Plan B would sacrifice some efficiency to gain more resiliency and diversity through distributed technology, thereby increasing agency and sovereignty. Why is there only one Internet Archive, Wikipedia, and Let's Encrypt, and why are they all in America? Our prior concerns about efficiency and duplication of effort should no longer be paramount.

This year, DEF CON will focus on agency, the ability of a citizen to have agency over their identity, data, and persona. We believe that supporting and choosing agency means respecting options when selecting which messaging apps, social media platforms, or email services you and your organization use, and that this will distinguish between what we have today and what is being built for tomorrow. If we consider policies and standards that incentivize individual agency, such as prohibiting high switching costs through data portability, we will encourage more innovative experiences in which users want to stay on a given platform, not because they are forced to through lock-in.

It won't be terribly expensive. Mastodon, a federated alternative to Twitter/X, is community supported.* Investments by NL Net Foundation helped create federated alternatives to both TikTok (Loops) and Instagram (PixelFed) by Daniel Supernault.** More agency-respecting options are built every day, but they lack the policy awareness many hyper-commercial competitors have.

By exercising their agency, hackers and researchers changed the language from "Responsible Disclosure" to "Coordinated Vulnerability Disclosure" (CVD) because companies held researchers hostage by claiming they were the bad actors should they ever disclose, even when the companies failed to correct their defects. Now the expectations are about coordination, not about who is more responsible than the other. Our involvement in these most foundational discussions to help guide our individual and collective agency will only become more relevant, as policymakers seek independent third party voices to better inform them about what is really happening in this next digital frontier.

*Mastodon. Accessed February 10, 2026. https://joinmastodon.org/.
**"Pixelfed." NLnet Foundation. Accessed February 10, 2026. https://nlnet.nl/project/Pixelfed/index.html.



ACKNOWLEGEMENTS & DIGITAL RESOURCES

ACKNOWLEDGEMENTS

Each year, a team of DEF CON technologists and Harris School of Public Policy graduate student volunteers works tirelessly to gather data, analyze top findings, and compile policy implications for cutting-edge insights. We are immensely grateful for their efforts and those of the DEF CON community as a whole, and we are especially indebted to the villages and other communities that bring eye-opening exploits to light year after year.

DEF CON *Franklin* and *The Hackers' Almanack* are especially grateful for:

- The organizers, subject matter experts, village leads, and partners from the broader DEF CON community who make the conference a reality each year;
- The support and contributions of Paul Chang, Divyansha Sehgal, Omar Ansari, Skyler Nunn, and Joshua Long, who helped capture many of the amazing findings from the DEF CON community;
- Mar Williams (spux.art), who designed and provided the visual theme for this year's report;
- The speakers featured in this report, who provided such illuminating content and also helped review and edit the *Almanack* (in order of appearance):

Keane Lucas, Joel Noguera, Diego Jurado, Tobias "ItsSixtyNein" Diehl, Lishuo "ret2ddme" Song, Ji'an "azraelxuemo" Zhou, Andrew "Helicopters of DC" Logan, Robert "LambdaCalculus" Menes, Quinn Dombrowski, James Utley, Jason Vogt, Josh Reiter, Roee Idan, Benjamin Mixon-Baca, Erlend Leiknes, Harrison Sand, Alex Holden, Thomas "fr0gger_" Roccia, John Fokker, Jon DiMaggio, Ben Folland, nyx, Reynaldo "buho", Victoria "V__Wave" Kumaran, Mark "LargeCardinal" Carney, John-Andre Bjørkhaug, Eaton Zveare, Marco Casagrande, Daniele Antonioli, Tung-Lin "Echo" Lee, Shang-De "HackerPeanutJohn" Jiang, Dong-Yi "Kazma" Ye, Leon "leonjza" Jacobs

- The University of Chicago Harris School of Public Policy, for providing resources to support this effort, and
- The Hacker Summer Camp community, which brings together so much great work.

DIGITAL RESOURCES

Artificial Intelligence: AI for Offense is Exploding, Yet Policymakers Remain in the Dark

- "Claude — Climbing a CTF Scoreboard Near You" video and blog post
- "Prompt. Scan. Exploit — AI's Journey Through Zero-Days And A Thousand Bugs" video and presentation
- "Mind the Data Voids: Hijacking Copilot Trust to Deliver C2 Instructions with Microsoft Authority" video and presentation
- "Safe Harbor or Hostile Waters: Unveiling the Hidden Perils of the TorchScript Engine in PyTorch" video and presentation
- "Voice Cloning Air Traffic Control: Vulnerabilities at Runway Crossings" video and presentation

Power: Down with Despots

- "Off-Grid Datarunning in Oppressive Regimes: Sneakernet and PirateBox" presentation
- "Bio-Cryptography is the Game-Genie in a Post Quantum Dystopia" video
- "Takes All Kinds: Building Onramps for Emergency Web Archiving in Ukraine and Beyond" video
- "Fighting the Digital Blockade: A View from Taiwan" video
- "Satellite Networks Under Siege: Cybersecurity Challenges of Targeted DDoS Attacks" video
- "TSPU: Russia's Firewall and Defending Against the Future of Digital Repression" video and presentation
- Meshtastic website

Cyber Crime: Hackers Don Cape and Mask

- "So Long, and Thanks for All the Phish" video and presentation
- "Killing Killnet" video and presentation
- "Where's My Crypto, Dude? The Ultimate Guide to Crypto Money Laundering (and How to Track It)" presentation
- "Ghosts of REvil: An Inside Look with the Hacker Behind the Kaseya Ransomware Attack" presentation
- "Man-in-the-Malware: Intercepting Adversarial Communications" video and presentation

Elsewhere, in the DEF CON Universe

- "Unmasking the Snitch Puck: the Creepy IoT Surveillance Tech in the School Bathroom" video and presentation
- "Diamonds Are For Hackers - Building the First Fully Open Source and Hackable Quantum Sensor" video
- "Pirates of the North Sea" video

Right to Repair / Irresponsible Companies / Disclosure

- "How API Flaws Led to Admin Access to Over 1,000 USA Dealers and Control Over Your Car" video
- "CTRAPS: CTAP Impersonation and API Confusion Attacks on FIDO2" presentation
- "Original Sin of SSO: macOS PRT Cookie Theft & Entra ID Persistence via Device Forgery" video and presentation
- "7 Vulns in 7 Days: Breaking Bloatware Faster Than It's Built" video and presentation

DEF CON website

University of Chicago Harris School of Public Policy - Cyber Policy Initiative website

The DEF CON 33 *Hackers' Almanack* is made possible with the support of:

craig newmark philanthropies

Mozilla Foundation

Thank you for reading the *Almanack*. Please follow our social media for the latest on DEF CON *Franklin*.



Website: https://defconfranklin.com/
Email: defconfranklin@gmail.com
LinkedIn: DEF CON *Franklin*
X, Bluesky, Threads: *@DEFCONFranklin*