

SHADOW & SIGNAL™ Newsletter

Fall 2026: My TEDx Talk Is Live, Plus Notes from a Full Season

Notes from the Edges of Technology, Intelligence, and National Security

A Note to Open

My TEDx talk, “Winning the Secret War for Your Mind,” is now online, and it is the best introduction I can offer to the work that has become my mission since leaving government. If you only have a few minutes for this issue, please spend them on the talk, and then share it with someone you care about.

The video went live last month, around the same time I opened the Deepfake Summit just outside Washington, DC. Both talks make the same case from different directions: your judgment has become one of the most valuable targets in the information age, and you have more power to defend it than you may realize.

Since the last issue, I also joined an embassy roundtable on transatlantic cyber defense and shared a stage with my husband for the first time. I published less than usual, because most of my writing hours went into research and early drafting for a book on Mind Sovereignty™. Please also read the fraud warning near the end of this issue. Criminals are still using my name and photo to defraud people, and I need your help to protect our friends and neighbors.

Here is the rundown.

FEATURED

Winning the Secret War for Your Mind



On the TEDxUF stage at the University of Florida, April 2026.



WATCH THE TALK

On the TEDx YouTube channel

youtu.be/sVWOFp21Tok or scan the code

I delivered this talk at TEDxUF at the University of Florida in April, and TEDx released the video on September 1. I wrote it for a general audience, so no background in national security is needed. It is the argument I have been building toward for some time, and the clearest short introduction to the book I am now writing.

The talk is about a contest for your mind that most people never notice. Foreign adversaries work to divide us and erode our trust. Meanwhile, the platforms we rely on every day compete for our attention by rewarding whatever stirs the strongest emotion. Both chip away at the same thing, our ability to think for ourselves, and the stakes reach well beyond any one of us, because a free society depends on citizens who can still form their own judgments.

I tell that story through my own career. It begins in a safehouse with a man who risked everything for the truth, and it traces how my early faith in freely flowing information met the very different world that algorithms have built.

“The algorithms don’t want you to know this, but they only have the power you give them.”

FROM “WINNING THE SECRET WAR FOR YOUR MIND,” TEDxUF

The talk is also practical. It closes with three habits drawn from intelligence tradecraft (Reclaim, Challenge, and Verify) and a quick three-question test called the S.P.Y. Check. Together they form the core of my Mind Sovereignty™ framework, and anyone can start using them today.

At its heart is one idea: in an age of algorithmic manipulation, the ultimate expression of freedom is thinking for yourself in a world designed to think for you.

If the talk resonates, please pass it along to someone in your family or at work, and write to tell me what you think. Your reactions will help shape the book.

On Stage This Fall

FORGED

THE DEEPPAKE SUMMIT | SEPTEMBER 1 | ARLINGTON, VIRGINIA

I opened the summit with a keynote titled “FORGED: Deepfakes and the Oldest Trick in Espionage.” The session began with a short video in which “I” asked the audience how they would know it was really me. I did not mention it again until midway through the talk, when I revealed that it was a deepfake assembled from my own public footprint. My case was that deepfake fraud follows the recruitment cycle intelligence officers have always used: spot a person with access, assess what motivates them, develop their trust, and ask them to act. An operation that once took months of one officer’s time can now be repeated across many targets at machine speed. The line I asked the room to remember was simple. Deepfakes are the disguise, and your judgment is the target. I closed with a recruitment pitch of my own, inviting everyone in the room to join the defense.

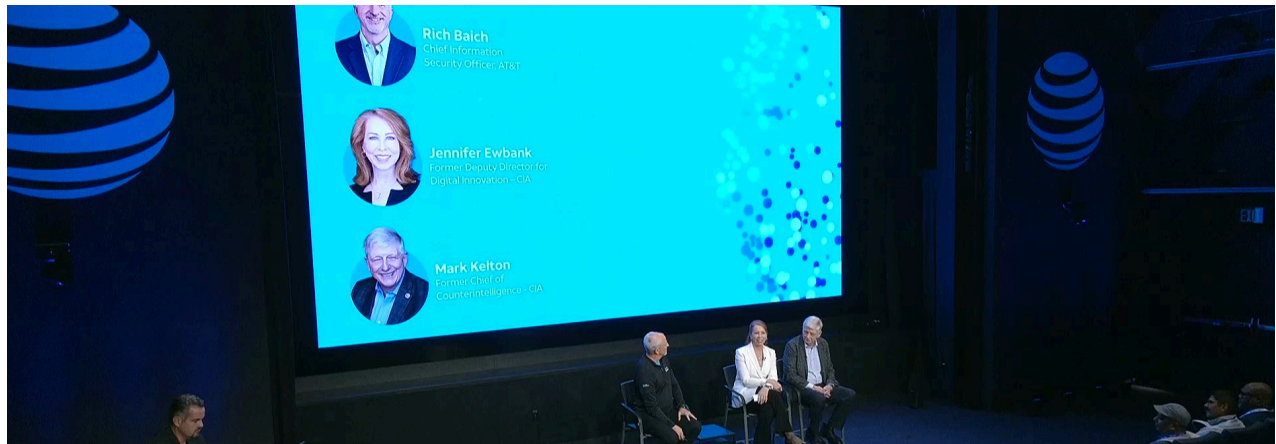
Cyber Threat Information Sharing Across the Atlantic

SEPTEMBER 9 | EMBASSY OF ESTONIA, WASHINGTON, DC

I joined a private roundtable convened by the Embassy of Estonia and the Cyber Security Forum Initiative (CSFI) on how allies can share cyber threat intelligence faster. Under the Chatham House Rule, I can share only my own view. The biggest barrier is speed. Attackers, increasingly aided by AI, have become dramatically faster, and the channels allies use to warn each other have not kept up. My recommendation was to decide before the next crisis what type of information gets released to whom, at what classification, and on whose signature, because those decisions take months to negotiate and seconds to apply. My thanks to CSFI founder Dr. Paul de Souza, Ambassador Hannes Hanso, Ambassador-at-Large for Cyber Diplomacy Helen Popp, and Dr. Anna-Maria Osula, who organized and moderated the discussion.

The Threat You Already Trust

OCTOBER 1 | AT&T SECURE CONNECTIONS, DALLAS



Rich Baich, Jennifer Ewbank, and Mark Kelton at AT&T Secure Connections in Dallas.

For the first time, I shared a stage with my husband, Mark Kelton, a retired senior CIA officer whose final assignment was chief of counterintelligence. Rich Baich, AT&T's Chief Information Security Officer and a former CIA CISO, moderated our fireside chat on insider threats. Mark brought stories from the Cold War spy wars, and I carried the conversation forward to North Korean IT workers hiding behind fake identities and to AI agents that organizations now need to treat as insiders. When Mark ended his introduction with "And we're married," the room erupted in laughter and applause, which was truly delightful and set the tone for the hour.

Three questions every leader should be able to answer

In the closing lightning round, Rich asked me for three questions a leader should be able to answer with real confidence about insider risk. Here is my answer.

- 1 What are your crown jewels, and what are all the paths to them?** Count the people, the connected systems, the software supply chain, and the AI agents that most organizations have not yet documented as identities.
- 2 How confident are you that each of those people and things is what it claims to be,** and that it still needs the access it has?
- 3 Would your team recognize an approach if someone made one,** and do they know whom to tell?

Away from the Stage and Keyboard

My board calendar has been full through the late summer and early fall, and the discussions have covered virtually every category of board governance we see in the news today. It's an honor to serve alongside a range of fellow directors and advisors, from whom I continue to learn so much.

In October, Mark and I joined the CIA Officers Memorial Foundation for its 17th annual Richard M. Helms Award Dinner, which carried special weight this year. It marked a quarter century since the September 11 attacks and since the Foundation was created in their aftermath to support the families of CIA officers who gave their lives in service to our country. The Foundation presented the Helms Award to Raul Fernandez, President and CEO of DXC Technology and Vice Chairman and co-owner of Monumental Sports & Entertainment, and honored FedEx founder Frederick W. Smith posthumously with the Patriot Award. It was a solemn and moving night, and I am proud to serve on the Foundation's board.

The Book

Most of my writing time this season went into research and early drafting for a book on Mind Sovereignty™. It grows directly out of the TEDx talk, which could only sketch the argument. Hostile states, criminals, and commercial platforms want different things from us, yet all of them work through the same algorithms, engineered to deliver content that spikes emotion so we act before we think. The book explains how that machinery works and offers practical tools for anyone who senses that something has gone wrong in our information environment. I hope to share more news in the months ahead.

What I've Been Writing

Because the book has my attention, I published less this season. Here are two pieces you may have missed.

Beijing's COVID-19 Blame-Shifting Campaign and the Long War on American Cohesion

My piece in Homeland Security Today on a China-linked social media network working to shift responsibility for COVID-19 onto the United States, how it fits Beijing's wider pattern of influence operations, and what Americans can do about it.

When Threats Move Faster Than Institutions

My piece in The Cipher Brief on the gap that defined the past year in national security: adversaries and their AI tools now move at machine speed, and the institutions meant to defend us are still built for human speed.

You can always find the latest on the [Shadow & Signal™ Blog](#) and on my [LinkedIn page](#), where I post shorter pieces once or twice a week.

CYBER AWARENESS

Someone Is (STILL) Pretending to Be Me

If someone using my name or photo contacts you through social media or a messaging app, it is not me. Please stop responding and report it.

Criminals continue to impersonate me online to defraud people, many of them older adults. Every so often, someone writes to tell me they have been contacted by a person using my name and picture. I am grateful to each of them for speaking up, and I am sorry for the worry these criminals cause.

I retired from government service in early 2024 and have no government role today. I do not investigate fraud for anyone, and I will never contact you to ask for money, account details, or personal information.

ic3.gov The FBI's Internet Crime Complaint Center

If you or someone you love is contacted:

- ◆ Stop responding, and do not send money or share personal or financial information.
- ◆ Report it to the FBI's Internet Crime Complaint Center at ic3.gov, with as much detail as you can. If you were asked to send money, include how and where, such as a cryptocurrency wallet address or QR code. FBI agents advise that these details help route a report to the right investigators.
- ◆ If you have lost money or feel threatened, contact your local police as well. You can also report fraud to the Federal Trade Commission at ReportFraud.ftc.gov.
- ◆ Type ic3.gov into your browser yourself. Scammers have begun impersonating the IC3 itself (!), and the IC3 says it will never contact you directly for information or money.

Please send reports to the authorities rather than to me, since I cannot investigate these cases or recover lost money.

This problem reaches far beyond one impersonator. According to the FBI's most recent annual Internet Crime Report, people age 60 and older reported losing more than \$7.7 billion to online fraud in 2025. Please share this note with the older adults in your life, especially those who spend time on social media.

COMING SOON

A New Website

I am in the middle of a full redesign of jennifer-ewbank.com. The new site will bring my speaking, writing, and board work together in one place. It will also be the home for future issues of this newsletter, which now lives on my website as a PDF you can save and share. Stay tuned.

Looking Ahead

The season is not over yet. In November, I'll deliver the keynote to a leading private equity firm's annual meeting. And in December, I will lead an interactive workshop on crisis communications and response for a large conference on the West Coast. My 2027 speaking calendar has some availability still, so if I can be of service to your event, your board, or your team, I would welcome the conversation.

Thank you for being here.

Jennifer Ewbank

Founder, Andaman Strategic Advisors
Former CIA Deputy Director for Digital Innovation

Speaking inquiries: Visit my [website](https://jennifer-ewbank.com) or [Leading Authorities, Inc.](https://www.leadingauthorities.com)

More at: jennifer-ewbank.com | [LinkedIn](https://www.linkedin.com/in/jenniferewbank)

Views expressed here are the author's alone and do not represent the positions or policies of the U.S. Government or the Central Intelligence Agency.