



Securing the Future: a talk with Jen Easterly on cyber threats, trust, and leadership in a digital world

15 May 2025, 11:39

Ann Debaere

In a world where disruption is inevitable, resilience isn't optional. It's essential. Few leaders understand this better than Jen Easterly, former Director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and decorated Army officer. Ahead of her keynote at Securing Tomorrow. Now., the Agoria & Sirris annual event on Wednesday, 4 June at Skyhall (Brussels Airport), we spoke with Easterly about leadership, cyber resilience, Europe's role in global security, and how businesses must adapt to a volatile digital future.

From your military and intelligence background, what lessons about resilience apply directly to business leaders?

Jen Easterly: One of the most important lessons is that resilience isn't just about bouncing back - it's about bouncing forward. It's about building the capacity to absorb shocks, adapt under pressure, and emerge stronger.

It takes more than preparation; it requires leadership, trust, and a strong culture. You can't prevent every disruption. Resilience means accepting that reality and preparing to respond and recover

with intent—through trained teams, resilient systems, and a clear mission mindset.

How do you view Europe's efforts to meet today's security challenges?



Jen Easterly, Former Director, U.S. Cybersecurity and Infrastructure Secure Agency

Jen Easterly: Cyberspace has no borders, and Europe has made meaningful strides, particularly in privacy regulation and harmonizing cyber policies. But the threat landscape is evolving faster than policies or bureaucracies can keep up.

We need speed, boldness, and collaboration—especially public-private partnerships across borders. Since threats are global, our defenses must be too.

Are there any threat scenarios still underestimated by leaders, especially in Europe?

Jen Easterly: Yes—particularly the long-term, strategic threats from nation-states like China and Russia. Cybercriminals are dangerous, but state actors present an even bigger risk. In the U.S., we've seen Chinese actors prepositioning themselves in critical infrastructure sectors. Also, artificial intelligence is a major risk vector—enabling more sophisticated cyberattacks, deepfakes, and disinformation. These risks aren't theoretical; they're happening now.

During your time at CISA, you led a major transformation. How did you modernize the agency?

Jen Easterly: When I joined CISA, we were a young agency facing massive hiring gaps—around 1,000 vacancies. We needed to build capacity and capability fast.

Beyond streamlining hiring, the real transformation was cultural. We created a mission-driven, people-centered culture that could attract top technical and collaborative talent. Trust—internally and with partners—was foundational.

What was one concrete measure you took to attract top talent?

Jen Easterly: Over my tenure, we hired over 2,200 people—not just technical experts, but collaborative ones. We focused on creating a workplace where people felt empowered, valued, and connected to a larger mission. In a competitive market, culture made all the difference.

Key quotes from Jen Easterly

- "Resilience isn't just about bouncing back. It's about bouncing forward."
- "You can't make a friend in the middle of a crisis. Trust must be built beforehand."
- "In cybersecurity, we need to stop glamorizing villains and start holding vendors accountable."
- "The burden of security shouldn't fall on users. It must be engineered in by design."
- "The future belongs to those bold enough to shape it, and securing tomorrow starts now."
- "Good cyber hygiene can prevent up to 98% of attacks. It's the basics that matter most."

What lessons from CISA, such as the Joint Cyber Defense Collaborative, could be applied in Belgium or Europe?

Jen Easterly: We created the Joint Cyber Defense Collaborative (JCDC) to break down silos between intelligence, law enforcement, and cyber defense agencies—and to work directly with the private sector.

This real-time, operational collaboration proved vital during crises like the Log4j vulnerability and the Russian invasion of Ukraine. Canada has since created its own version. I believe Europe could benefit from a similar model—not just nationally, but across the EU.

As I often say: you can't make a friend in the middle of a crisis. Trust and cooperation must be built beforehand.

How should international cooperation evolve to match the borderless nature of cyber threats?

Jen Easterly: We need real-time operational collaboration, not just alliances on paper. In the U.S., cybersecurity has been elevated to a national security imperative with serious leadership focus and funding.

Europe has many strong elements but would benefit from greater unity of effort across national capabilities. An integrated EU-wide approach, with strong ties to the U.S. and allies, will be critical



n'
fferently?

Jen Easterly: We glamorize villains like Volt Typhoon and blame victims for not patching systems—but we need to shift the focus to holding technology vendors accountable.

Security must be a core design feature, prioritized by CEOs, boards, and product teams from day one. Speed-to-market and cutting costs have often been prioritized over security—and that has to change.

We launched a Secure by Design pledge, and over 300 companies have signed it. Europe is leading with initiatives like the Cyber Resilience Act, pushing for higher security standards faster than the U.S.

You wouldn't buy a car today without seatbelts. Likewise, we shouldn't accept digital products without basic built-in protections.

How can manufacturing companies better balance innovation with cybersecurity?

Jen Easterly: Innovation is essential, but security must be built in from the start. Manufacturing companies must understand their "crown jewels"—critical systems and data—and protect them with layered defenses and network segmentation.

Too often, cybersecurity is seen as an insurance policy. It should be treated as a core investment, alongside innovation and productivity. Companies must use their purchasing power to demand better security from their vendors.

For smaller companies without the resources of large enterprises, what are the top three cybersecurity priorities?

Jen Easterly:

1. **Install updates:** Many attacks exploit known vulnerabilities that updates would fix.
2. **Use strong passwords and a password manager:** Unique passwords are critical.
3. **Think before you click:** Train employees to be cautious about emails, texts, and calls.

Also, enable multi-factor authentication (MFA). These basic steps—cyber hygiene—can prevent up to 98% of attacks.

What concrete steps can leaders take to embed cybersecurity across their organizations?

Jen Easterly:

- **Make it personal:** Connect actions to real-world risks through storytelling, not fear-mongering.
- **Lead from the top:** CEOs and boards must treat cybersecurity as a leadership responsibility, not an IT problem.
- **Celebrate security:** Recognize and reward secure practices across the organization.

It's about cultural change—and leaders must both talk the talk and walk the walk.

Finally, why should Belgian business leaders attend "Securing Tomorrow. Now." and hear your keynote?

Jen Easterly: Because the future is being written today, and it belongs to those bold enough to shape it. The threats are urgent, but so is the opportunity to build a safer, stronger digital world.

In Brussels, I'll be sharing lessons from the front lines, on leadership, resilience, and securing our future. I'm not just coming to inform; I'm coming to inspire.

Authors



Ann Debaere