SPEAKER ONE-SHEET

Trevor H. Rudolph

The intersection of geopolitics, national security, and technology

White House CNAP Architect & Fortune 500 Government Affairs Executive
Brussels & Washington, DC



SPEAKER BIO

Trevor H. Rudolph has spent his career at the exact point where government power meets global technology — first building it, then translating it for the companies who have to live with it. As Chief of the Cyber and National Security Unit at the White House Office of Management and Budget, he built the federal government's first-ever cybersecurity oversight function from scratch and served as lead architect of President Obama's Cybersecurity National Action Plan, securing a historic $19 billion investment and driving a 30% jump in multi-factor authentication across the federal government in just 30 days. He later built Schneider Electric's first global government affairs and technology policy function from the ground up, turning the EU's toughest new cyber rules — NIS2, the Cyber Resilience Act — into competitive advantage for a Fortune 500 multinational, work that won the 2024 ITI International Advocacy Award.

Now based in Brussels as a Senior Non-Resident Fellow at the Atlantic Council's GeoTech Center, Rudolph sits inside the rooms where U.S. and EU technology policy actually gets made — briefing officials across the U.S. government, the European Commission, and the European Parliament, and publishing on the EU's “Digital Sovereignty Triad” and transatlantic tech policy for the Atlantic Council and Tech Policy Press. He brings audiences a rare, dual-sided fluency: the instincts of a government insider who wrote the rules, and the operating experience of a corporate executive who had to comply with them — delivered with the on-camera ease of someone equally at home on C-SPAN, Al Jazeera English, Sky News, and the RSA Conference stage.

SIGNATURE TALKS

The Regulatory Gauntlet: Turning Global Cyber Compliance Into Competitive Advantage

For corporate, association, and industry audiences navigating the EU's NIS2, Cyber Resilience Act, DORA, and AI Act — alongside the non-EU rules that collide with them: U.S. National Defense Authorization Act Section 889, U.S. Commerce Department Entity List designations, China's Unreliable Entity List, and China's Cybersecurity Law, Data Security Law, and Personal Information Protection Law. Drawing on his experience building Schneider Electric's award-winning global policy function, Rudolph shows executives how to stop treating regulatory pressure as a cost center and start using it as a market differentiator — with a concrete playbook for aligning legal, security, and government affairs teams before the next rule lands.

Great-Power Tech Competition: What U.S.–China Rivalry Means for Industry

For corporate, investor, and policy audiences. Rudolph explains how Washington and Beijing's contest over technology — export controls, entity listings, data and supply-chain rules, and the race for AI and semiconductors — lands on companies caught in the middle, and how to read the signals, manage the risk, and plan for a world of competing technology blocs. Informed by time inside the U.S. government and by years running government affairs for a multinational that had to operate on both sides of the divide.

Avoiding Digital Divorce: Sovereign Clouds and the Threat of a U.S. Kill Switch

For government, critical-infrastructure, and technology audiences. As governments push for sovereign clouds, a hard question follows: what happens if access to foreign-controlled technology can be switched off? Rudolph, who presented on this at GovWare Singapore, examines how geopolitics is reshaping cloud and infrastructure decisions — and what governments and companies can do now to reduce dependency without splitting the digital world apart.

Inside the Situation Room: What the White House Taught Me About Leading Through Crisis

For leadership, government, and cybersecurity audiences. Before the age of 40, Rudolph helped lead the federal response to the OPM data breach — an attack with a clear espionage element — and the Cybersecurity National Action Plan that followed, including the 30-day sprint that lifted multi-factor authentication 30% across the federal government. He draws out transferable lessons on decision-making under pressure and mobilizing large organizations fast, and recounts how the story followed him to Beijing in 2018, where Chinese government officials, meeting him in his Schneider Electric role, had compiled a dossier on him and wanted to put their questions to him alone.

Anatomy of a Breach: What the OPM Hack Teaches Us About Cyber Conflict in the AI Era

For university, security, and government and corporate audiences. Rudolph, who directed the federal response, walks step by step through the 2014–15 OPM intrusion — a stolen contractor credential, valid logins that looked like normal traffic, and about eleven months undetected — then examines why China-linked actors wanted personnel data, why Washington treated it as espionage rather than an act of war, and what that line means for deterrence. He closes by fast-forwarding to 2026, where the same weak points of identity, third-party trust, and slow detection meet attackers and defenders operating at machine speed with AI. Built to be interactive, with audience discussion breaks.

The Digital Sovereignty Triad: What Europe's Tech Rules Mean for Every Global Business

For international business, trade, and technology audiences. A field guide to the EU's expanding ambitions over data, infrastructure, and AI — and what it actually means for any company operating on both sides of the Atlantic — from a speaker who advises EU and U.S. policymakers on both sides of that divide.

VIDEO PORTFOLIO

Representative clips from panels, moderated sessions, and Trevor's interactive geopolitics talk show:

Speaking reel (2 minutes)
https://youtu.be/EcfMNrIh_uk
Moderating, hosting and analysis, including the 2026 World Emerging Security Forum in Seoul and Memo: Random.

“Memo: Random” Episode 1: The Trump-Xi Summit in DC (Condensed Version)
https://youtu.be/9sJSHP_-DK0
Condensed first episode of Memo: Random, an interactive geopolitical talk show hosted by Trevor, with guest Naomi Wilson of ITI.

Tech Triangle: AI, Cyber, and Nuclear — World Emerging Security Forum, Seoul
https://www.linkedin.com/feed/update/urn:li:activity:7506354972469485569/
Trevor moderating the Tech Triangle panel at the 2026 World Emerging Security Forum.

“The Impact of Regulation on Multinational Companies” — S4, with Dale Peterson and Ryan Rathbun
https://youtu.be/rEObl78WJLE

“Can Europe Take Over the Digital World?” — CGTN Europe
https://youtube.com/shorts/GaPEsNV2UlM
Digital sovereignty panel highlight (short-form clip).

SELECTED STAGES & MEDIA

- RSA Conference (2016, 2025)
- IQT The Hague (2024)
- U.S. Chamber NOW+NEXT Conference
- GovWare Singapore Cyber Week
- World Emerging Security Forum
- C-SPAN, NextG (2016)
- ABC News
- Al Jazeera English
- Sky News
- Politico & Federal Computer Week
- ITI “Download on Tech” podcast

info@rudolphventures.com | +32 496 55 06 96 | rudolphventures.com | Based in Brussels, Belgium
linkedin.com/in/trevor-h-rudolph | linkedin.com/company/rudolph-ventures