

VISION ON CYBERSECURITY AND WHAT IT MEANS FOR IT PEOPLE

SAI 2025

Chris Kubecka de Medina, CEO HypaSec, The Hacktress

PRESENTER

- The Hacktress
- Almost US Defense Science Board Member
Generative AI & Cyberwarfare
- Cyber warfare incident management
EMEA, governments
- Critical infrastructure security: Oil & Gas, Water,
Maritime, Aviation, Energy & Nuclear
- Former Head of Aramco Information Protection
- Former U.S Air Force Aviator & Space
Command-Command & Control Systems



How A 10-Year-Old War Dialer Became A Top Cybersecurity Expert

THE FUTURE HAS ARRIVED

- Cybersecurity = national stability
- IT professionals = frontline defenders
- Threats now blend digital + physical
- Quantum & AI accelerate everything
- The next decade is decisive

WHAT HAS CHANGED

- AI-driven cyber operations & misinformation
- Hybrid warfare across Europe
- Authoritarian digital coercion
- Drones, robotics, and the space–cyber domain
- Quantum computing (PQC transition era)

MY VISION: THE NEXT CYBER DECADE

- Cyber risk becomes geopolitical
- AI transforms offense and defense
- PQC transition becomes mandatory
- Cyber + physical merge into one domain
- Resilience becomes the core strategy

QUANTUM ERA REALITY

- RSA/ECC will fall
- Harvest Now, Decrypt Later is active
- PQC migration takes years
- Crypto-agility becomes essential
- Encryption becomes a national asset

CRYPTOGRAPHY BECOMES A GEOPOLITICAL ASSET

- The Future of Cybersecurity
- Most nations are unprepared for the PQC transition. Quantum will not arrive gently; adversaries will weaponize uncertainty long before capability.

ACADEMIC ARTICLE FREE/OPEN

- **Secrets From the Future:
Hacking in a Post-
Quantum Cryptography
World: Implications for
Cyber Security and
National Defense**



AI TRANSFORMS CYBER WARFARE

- AI automates reconnaissance
- AI generates phishing & deepfakes
- AI agents can run attacks
- Misinformation becomes a weapon
- Truth becomes part of security

MOLDOVAN CYBER DIRECTORATE



HYBRID WARFARE EXPANDS

- Cyber + sabotage + drones
- Attacks on grids, ports, aviation
- Election interference & influence ops
- Info-ops against civil society
- Space-cyber becomes a target

AUTHORITARIAN DIGITAL COERCION

- Surveillance + AI intimidation
- Targeting journalists & dissidents
- Diaspora pressure & data leaks
- State–criminal alliances
- Coercion without firing a shot

WHAT THIS MEANS FOR IT

- Your role is now societal security
- Defending infrastructure, not just networks
- Managing PQC transition
- Handling AI-era threats
- Protecting democracy itself

SHIFT TO RESILIENCE ENGINEERING

- Systems must survive attacks
- Rapid recovery > perfect prevention
- Segmentation + blast-radius control
- Crypto-agility built-in
- Continuous operations under stress

CYBER + PHYSICAL FUSION

- Drones = flying computers
- ICS/OT attacks = real-world damage
- Satellites = new cyber targets
- Robotics in conflict zones
- IT needs physical-world awareness

EUROPE IS ON ITS OWN

Compliments of 🍌.

Geauga County, Ohio, YMCA....



HUMAN SKILLS BECOME CRITICAL

- Judgment beats automation
- Strategy beats tooling
- Ethics beats efficiency
- Geopolitical awareness matters
- Communication = core skill

THE NEW IT PROFESSIONAL

- Bridge between tech & leadership
- Defender of infrastructure
- Guardian of digital identity
- Interpreter of hybrid threats
- Architect of resilience

PRACTICAL CALLS TO ACTION

- Inventory + replace vulnerable crypto
- Adopt crypto-agile architectures
- Train for hybrid warfare recognition
- Integrate AI-aware defenses
- Protect people, not just systems

CLOSING VISION

- Cybersecurity is now human security
- IT professionals shape national resilience
- Democracies depend on your work
- The challenge is immense
- So is your impact

THANK YOU & QUESTIONS

- Thanks to everyone with the SAI
- Marc Vael thank you!
- @SecEvangelism on Social media
- Thank you for listening

