WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
GREECE

W4C GR CYBERSECURITY WOMAN PROFILE OF THE MONTH

INTERVIEW WITH ZOEY!

Name: *Zoey Stambolliu*
Job Position: *Director, Government Affairs & Cybersecurity Policy,Europe*
Current Employer: *Mastercard*
Cybersecurity areas of expertise: *Public Policy*
Previous career(s): *Senior Policy Manager for Cybersecurity Policy at DIGITALEUROPE*
Educational background:
· Master's in European Politics and Governance from the College of Europe in Bruges, Belgium
· Bachelor's in International and European Affairs from the University of Piraeus in Greece
Other interests/hobbies: *painting, Pilates*
Favourite quote: *"Success is not final, failure is not fatal: it is the courage to continue that counts" - Winston Churchill*
Network with me: *Zoey Stambolliu | LinkedIn*

Intro & Inspirational

1. Which values are guiding your life and work?

Integrity, resilience, and empathy are the guiding pillars of both my personal and professional journeys. In cybersecurity policy, integrity means making decisions that hold up to scrutiny, prioritising transparency and the public good. Resilience is essential when facing setbacks or rapidly changing threats—a quality I nurture not only at work but in life. Empathy allows me to understand diverse perspectives and foster inclusive, effective teams. Upholding these values ensures my work is meaningful and my relationships are built on trust.

2. What's the most important life lesson you've learned?

The most important lesson I have learned is that courage matters more than certainty. In both my career and personal life, stepping into the unknown and persevering through challenges has been far more valuable than waiting for perfect conditions. As Winston Churchill said, "Success is not final, failure is not fatal: it is the courage to continue that counts." This mindset has helped me embrace change, learn from failure, and push boundaries.

3. How do you define success? And what's the best advice that you can give about success?

To me, success is the ability to make a positive impact on others, continually learn, and remain true to your values. My best advice is to view success as a journey, not a destination. Celebrate progress, learn from setbacks, and always stay curious. Surround yourself with people who inspire you, and remember that your unique perspective is your strength.

4. Do you think your job makes a difference? How?

Absolutely. As a director for cybersecurity policy, I have the privilege of shaping frameworks that protect people, organisations, and digital ecosystems. The work we do safeguards the society, builds trust in technology, and empowers individuals to thrive in a digital world. Every policy, dialogue, and initiative has a ripple effect, contributing to a safer and more inclusive future.

5.What is the best and the worst piece of advice you received? (+How did you unlearn the latter or use it to your favour?)

The best advice I received was to never underestimate the power of authentic connections; building genuine relationships opens doors and fosters collaboration. The worst advice was to "stick to your lane." Early in my career, I was told to focus narrowly on my role and avoid venturing beyond it. I unlearned this by embracing interdisciplinary approaches and seeking out opportunities to broaden my perspective. Growth often comes from stepping outside comfort zones, and today I encourage others to be curious and explore new horizons.

6.Can you name a book that has influenced your journey?

One book that has profoundly influenced my journey is Desert Flower by Waris Dirie. Her story is a testament to the power of resilience and the importance of standing up for what you believe in, even in the face of significant adversity. Waris Dirie's remarkable journey and unwavering determination have inspired me to embrace challenges with courage, and to truly value the resilience that women demonstrate in the face of adversity. Witnessing such examples has encouraged me to stand firm, use my voice, and uplift others, both within cybersecurity policy and beyond. Thanks to the inspiration of women like Waris Dirie, I have learned to appreciate the importance of perseverance, solidarity, and the power of advocating for positive change—even when the odds seem insurmountable.

Cybersecurity General

7. How can someone stand out in a competitive cybersecurity job market?

Standing out begins with building a personal brand anchored in authenticity and continuous learning. Practical experience—whether through internships, volunteering, or personal projects—demonstrates initiative and real-world problem-solving. Tailor your CV and cover letter to highlight not just technical achievements, but also examples of teamwork and adaptability. Engage with professional communities, attend industry events, and share your insights online. Employers notice candidates who are curious, proactive, and able to communicate complex ideas simply.

8. What trends in the technology & cybersecurity industry are you keeping an eye on for the future?

I'm closely watching the growing impact of artificial intelligence and machine learning on both attack vectors and defence strategies. The increasing regulatory focus on data privacy and digital autonomy is also important. Additionally, the expansion of the Internet of Things and remote work introduces new risks and opportunities. Keeping pace with these trends requires a commitment to learning and an open mind about how technology is reshaping our world.

9. What is the most common mistake someone could make when applying for a role in the cybersecurity industry? What do you believe makes a successful candidate/application?

A frequent mistake is submitting generic applications that don't reflect a genuine interest in the specific organisation or role. Candidates sometimes overlook the importance of soft skills, focusing solely on technical qualifications. A successful application clearly connects your experience and passion to the company's mission, demonstrates research into their work, and showcases both technical and interpersonal strengths.

10. Do you believe that there are misconceptions people make about working in the cybersecurity industry?

Many assume cybersecurity is only for technical experts or that it's an isolating, high-pressure field. In reality, the industry offers a wide variety of roles—from policy and risk management to communications and legal—suiting diverse skillsets. There's also a misconception that work-life balance is unattainable, but with supportive teams and flexible practices, a healthy balance is possible. The field is far more collaborative and creative than often believed.

11. Which concrete recommendations would you give to women who want to change career and join cybersecurity?

Recognise and embrace your transferable skills—such as problem-solving, communication, and leadership—which are highly valued in cybersecurity policy. Seek out networking opportunities, whether through women-in-tech groups, conferences, or online forums, to build confidence and find mentors. Don't be deterred by a lack of traditional technical experience; the industry needs varied perspectives and backgrounds. Be bold in applying for roles, even if you don't meet every requirement on paper.

12. And any tips for those who are still very young and might be considering it? Can they start "preparing" somehow from early on?

For young people considering cybersecurity from a public policy angle, early preparation is less about technical specialization and more about building strong foundations. An interest in how technology affects society, basic digital literacy, and exposure to policy debates, international relations, or governance issues are all valuable. Learning to write clearly, assess evidence, and understand trade-offs early on is especially important for policy careers.

13. What skills do you think are not "most important", as this is very limiting, but skills that are key for a career in cybersecurity no matter the specific profile?

Across cybersecurity policy roles, a few core skills matter consistently: systems thinking, critical judgment under uncertainty, and the ability to translate technical risks into policy and regulatory implications. An understanding of ethics, public interest, and geopolitics is essential, as is adaptability—because technology, threats, and policy frameworks evolve quickly. These skills are relevant regardless of the specific cybersecurity policy profile.

14. Do you (or did you) have a mentor or someone who guided you? What is your opinion on mentoring as well as on getting a start via an internship/traineeship? Are you planning to mentor or coach others in the future, or have you been mentoring already?

I've been fortunate to have mentors who encouraged me to stretch beyond my comfort zone and offered invaluable perspective. Mentoring accelerates learning, builds confidence, and fosters a sense of belonging—especially for those new to the industry. Internships and traineeships are excellent ways to gain hands-on experience and build networks. I am actively mentoring and plan to continue, as supporting others is both a privilege and a responsibility I value deeply.

You & Your job

15. What was your childhood dream job (and why you liked it)?
I wanted to be a diplomat-slash-detective—someone who solved big problems by talking to people and reading between the lines. I was fascinated by how decisions made in one room could ripple outward and affect millions. In hindsight, cyber policy is exactly that, just with more acronyms and fewer trench coats.

16. Did peer pressure, trends or other factors play a role in your choosing cybersecurity and particularly your specific field of work in it?
There was definitely a moment when "cyber" went from niche to unavoidable. Every crisis, every geopolitical conversation suddenly had a digital layer. What pulled me in wasn't hype, though—it was the realization that no government can secure cyberspace alone. Public-private partnerships across Europe felt like the hardest problem in the room, which usually means it's the right one to work on.

17. Did you face any challenges related to your gender, race, visual appearance, or background, or any stereotypical biases? How have you overcome these?
Being the only woman in the room—or the only non-technical background—can make assumptions travel faster than facts. I learned early on to be very well prepared and only moderately patient. Over time, credibility compounds. Once people see you can translate between policymakers and engineers without losing either side, the stereotypes tend to get bored and leave.

18. Do (did) you ever experience imposter syndrome and self-doubt about your career and skills?
Yes, but I've learned to treat imposter syndrome as a sign that I'm operating at the edge of my comfort zone—which is usually where the interesting work is. Also, it helps to remember that everyone else is quietly Googling things too.

19. Do you enjoy your work, and why? What's your favourite and least favourite part of your job?
I genuinely love it. My favourite part is building trust between sectors that don't always speak the same language—governments, companies, and civil society. When that clicks, real progress happens. Least favourite part? Meetings that could have been emails.

20. What role has networking played in your skill development?
Networking has been essential—not in the transactional sense, but in the "who do I call when something breaks at scale?" sense. Cybersecurity in Europe runs on relationships. Every coffee, panel, or even cyber exercise has taught me something new, often faster than any formal training. Skills grow, but networks make them usable.