

TOP CYBER NEWS MAGAZINE

NOVEMBER 2024



QUANTUM SECURITY
with JAMES CASTLE



The Strategic Leaders' Perspectives

on Emerging Trends

Fore Word

At **Top Cyber News MAGAZINE**, we engage with people every day. This systematic and interconnected exchange of information, ideas, and strategies has brought forth true diamonds: the genuine talents of inspirational experts..

Amid the global cyber-skills shortage, it becomes imperative to celebrate talent dedicated to cybersecurity - those who invest their energy and careers into this vital field.

And then... among these wonderful professionals, there are individuals whose excellence cannot be captured by a one-page storyline. There are experts whose story is a 'Nova': "*Stars that become Nova's and are nearly always too faint before eruption to be seen with the unaided eye. Their sudden increase in luminosity, however, is sometimes great enough to make them readily visible in the nighttime sky.*"

James Castle - the *Godfather of Quantum Security* graces our November 2024 edition! A role model who leads the way for countries, continents, and generations. Celebrate this talent! Brighten the light in others, and you will be amazed by how that radiance returns to you! Enjoy reading, sharing, and learning!

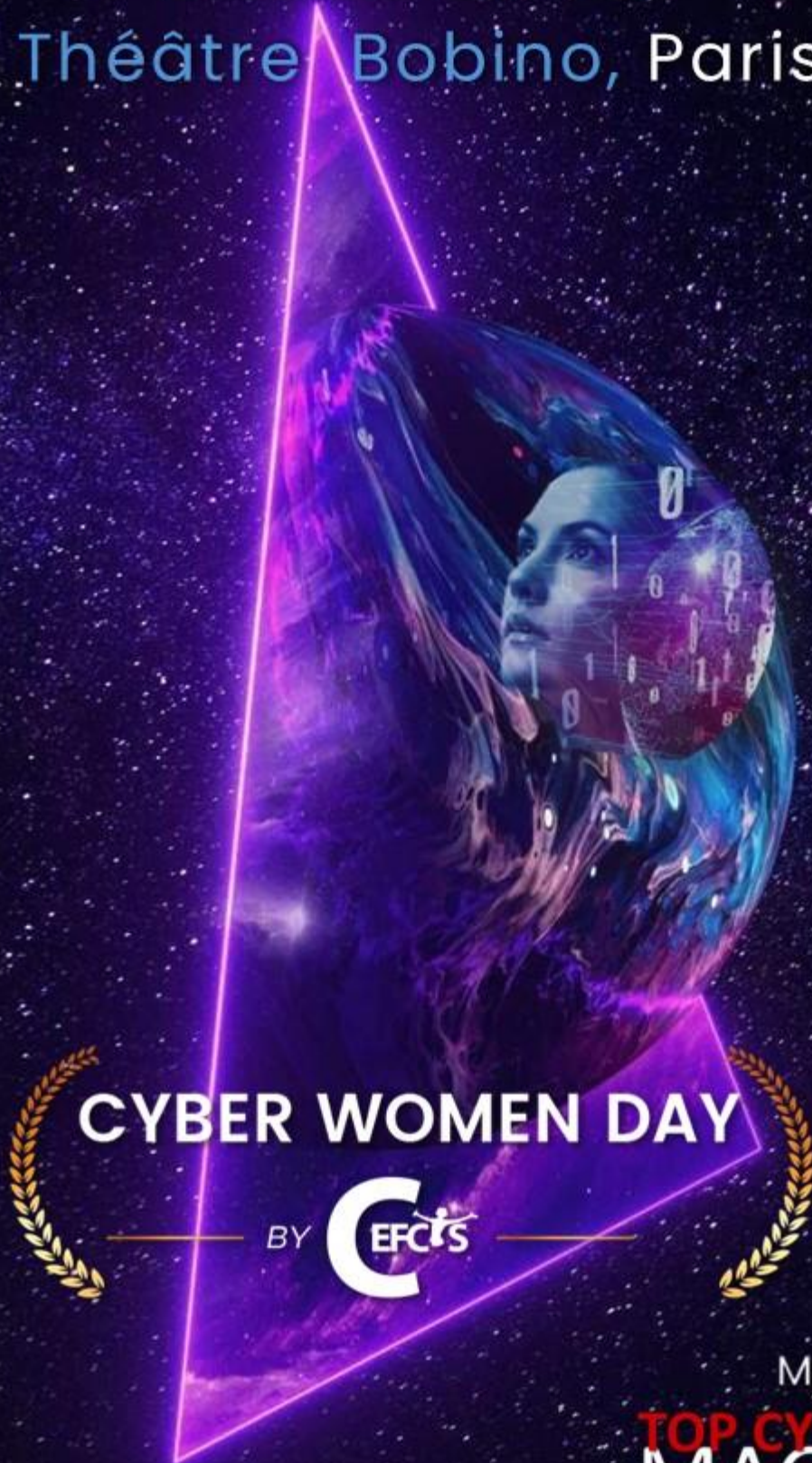
Integrating Excellence With The Future!
Top Cyber News MAGAZINE

The European CyberWoman Excellence Awards!

#EuropeanCyberWomenDay

December 10th, 2024

Théâtre Bobino, Paris



CYBER WOMEN DAY

BY



Media Partner

**TOP CYBER NEWS
MAGAZINE**

Future of Interconnectivity

Editorial by **Alex Keedy**, United States

As the world continues to become more interconnected by the digital fibers weaving us together, we continue to uncover just how vulnerable we are to crippling cyber attacks. Every day consumers of the internet who wish to be naïve to the threats lurking on dark web marketplaces have now found themselves terrified as they cannot escape news media broadcasting high-profile attacks affecting citizens. Whether it was the result of attacks leading to limitations at the gas pump or attacks impacting power grids leaving people without electricity for hours, the world is starkly aware of how cyber is not just a new and separate industry anymore; it is an inherent basic necessity of every industry.

We need cybersecurity and the cyber warriors to defend every person who relies on the Internet to keep their industry going.

To combat these threat actors, we must first understand them and their operations. *Many of the financially-motivated ransomware groups operate efficiently like a well-oiled Fortune 500 company, with help desk lines, affiliate program payouts, and training teams.* By studying their behaviors instead of focusing on atomic indicators, we can be more proactive in identifying behavior that might indicate malicious intent. Cybercrime experts have observed prolific actors like fooble or pompompurin serve as initial access brokers that sell various types of corporate access such as VPN, RDP, AD etc credentials to other cybercriminal groups who commit other nefarious acts against victims. *Cybercriminals have undoubtedly demonstrated that they share, and broker information so why don't we also do so?* Only by cooperation and intel-sharing between both the private and public sector will we be able to make considerable strides in making the digital world safer for everyone.

I implore all cyber leaders to share essential intel as we're all working towards a safer digital world.



40 under 40 in Cybersecurity by Top Cyber News MAGAZINE, Cyber Threat Intelligence Expert, **Alex Keady**, is currently **Flashpoint's Senior Strategic Advisor**. Flashpoint is the leader in threat data and intelligence. Alex's background in cybercrime investigation focused on Ransomware-as-a-Service groups and enablers such as initial access brokers.

She achieved a **Master's degree in International Relations** with a focus in intelligence studies and a **Master's in Business Administration** from the **Johns Hopkins Carey Business School**. Alex was nominated for "Next Generation Leader of the Year" at the September 2022 Women in Technology International Award Ceremony.

A portrait of James Castle, a middle-aged man with short grey hair and glasses, wearing a dark suit, white shirt, and dark tie. He is smiling slightly. The background is a dark blue with a glowing, abstract pattern of light blue dots and lines, resembling a digital or quantum theme. A vertical dashed white line is on the left side of the image.

James Castle, Toronto, Canada

James Castle - the Godfather of Quantum Security is the Executive Director and Founder of Cyber Security Global Alliance (CSGA), a non-profit organization established in April 2021. CSGA was created with a small group of co-founders during the COVID-19 pandemic with the mission of uniting small and medium-sized businesses (SMBs) to collaborate and develop joint cybersecurity solutions. Through CSGA, we aim to defend our nation against a range of threats, including the rising danger of modern-day ransomware and the future challenges posed by post-quantum ransomware.

James Castle & Cyber Security Global Alliance 360



Cyber Security Global Alliance (CSGA), is the legal operating name for Terranova Defense NFP (Not-For-Profit). Terranova Defense NFP is a federally incorporated non-profit membership-based non-governmental organization. As the operational lead for global cybersecurity initiatives, CSGA works alongside the Terranova Defense Group of Companies to address critical infrastructure security and digital resilience. By fostering collaboration and partnership, we provide the resources needed to reduce risks to global cyber and physical infrastructure outside the United States.

CSGA is proud to announce that CSR5's software-based ransomware protection is now available, offering enhanced protection for businesses and their digital presence. *We are committed to providing innovative solutions to safeguard companies against ransomware attacks and other cybersecurity threats.*

In addition to our cybersecurity services, CSGA offers a wide range of expertise in Quantum Security, Quantum AI, Cyber Education, Cyber Awareness, Cyber Mentoring, Cyber Defense, and Cyber Artificial Intelligence.

Our global defense strategy focuses on diversity and inclusion, empowering businesses to navigate the complexities of the digital landscape while driving increased profitability and productivity.

As part of our ongoing efforts to recognize excellence in cybersecurity, Cyber Security Global Alliance (CSGA) partners with Top Cyber News MAGAZINE and CSB.school (France) to host the "Top International 40 Under 40 in Cybersecurity" Recognition Program, honoring individuals under 40 who have made significant contributions to the cybersecurity field since 2022. This program was founded by Editor in Chief Dr. Ludmila Morozova-Buss.

With one of the world's largest cyber defense hubs, Cyber Security Global Alliance is committed to addressing internal threats and cyberattacks, providing businesses with the tools and knowledge to stay ahead of digital threats. Our partnership with CSR5 Global Incorporated, will be launching our joint groundbreaking technology on December 1, 2024, that will revolutionize how businesses approach cybersecurity through quantum and blockchain security.

Additionally, James Castle and his team will be launching the Cybersecurity Immersion and White Hat Program in partnership with the Borough of Manhattan Community College on January 1, 2025. This program will replace traditional college and university cybersecurity education with an innovative 100% online learning experience developed by Socratic Arts, supported by program mentoring and practical business education delivered by the Barr Business School.

James Castle also serves as the CEO of Terranova Aerospace and Defense Group (USA), overseeing divisions in Quantum Security, Quantum Defense, Quantum AI, Cybersecurity, Cyber Defense, Aerospace, Maritime, and Communications.

The Terranova Aerospace and Defense Group is working with their U.S. partners on new radar-based technology that can now assist in weather navigation in real time that can service search and rescue, and emergency responder operations in lifesaving operations, recently tested in the United States on the Eastern Seaboard 2024. James leads global teams and collaborates with domestic and international companies to mitigate physical and digital threats, ensuring the continuous flow of commerce and access to critical services.

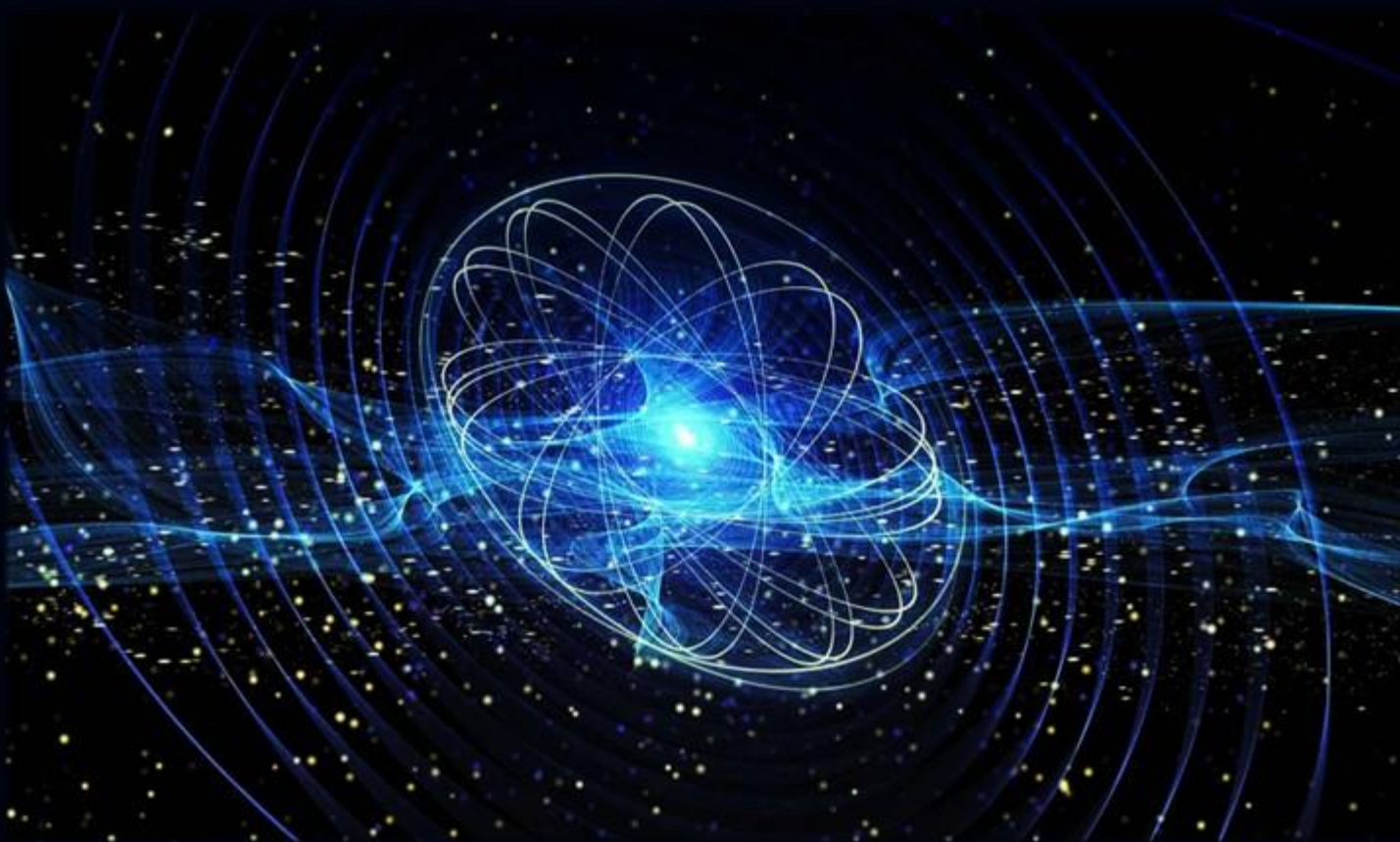
James has been recognized as a global defense visionary and a leader in strategic partnerships, cybersecurity advancements, and corporate growth. James has been recognized as an Industry Game Changer and has been a Canadian Ambassador to an EU Commission Think Tank called Drone Think Do for over a decade, representing thousands of companies throughout 64 countries globally. His company, *Terranova Defense, has been acknowledged as one of Canada's Top 100 Defense Companies and endorsed by the U.S. Department of Commerce for its contributions to cyber defense.*

Continuing his commitment to global defense, James Castle remains focused on advancing cybersecurity initiatives and pushing the boundaries of innovation through partnerships, research, and technology development.

James Castle is the Godfather to Quantum Security and Champion of Cyber Threat Prevention

Since the creation of Post-Quantum Security, companies and organizations have raced to be the next Cyber Defense Guru. This whitepaper summarizes and directly looks at the pros and cons of post-quantum security and focuses on the key technologies that will prevent Ransomware, and current cyberattacks that threaten the global defense initiative.

Today, humanity is faced with many obstacles that have slowed down our resolve of cyber threats and in the prevention of cyberattacks. In Canada, cybersecurity legislation has slowed down the process of prevention and mitigation that makes enforcement almost impossible from being achieved. Terranova and CSGA quantum and security experts identify what this means for humanity and the current digital age. James Castle continues to focus on these key variables ranging from basic quantum security to the ongoing threats of cyber terrorism and global warfare with the means to stand fast against cyber threat and threat actors globally.



What is Quantum

A discrete, indivisible manifestation of a physical property, such as a force or angular momentum. Some quanta take the form of elementary particles; for example, the quantum of electromagnetic radiation is the photon, while the quanta of the weak force are the W and Z particles. Even though the definition of Quantum means very little to humanity's understanding on Quantum, it is important to understand that this is a new technology that needs to be defined and to identify the future elements that make this technology possible, and through James Castle, Executive Director and Founder of Cyber Security Global Alliance (CSGA), we will help our readers find that definition with a basic understanding of why quantum technology exists and why it's so important to our future.

As technology continues to play an increasingly vital role in our lives, so does the need for data protection and digital security. With cyber-attacks on the rise, it's essential to take measures to stay safe. That's where the CSR5 comes in.

CSR5 - Global Threat Response Software is revolutionizing the cybersecurity industry with its wholistic cybersecurity service platform. Backed by one of the world's largest cyber defense hubs: Cyber Security Global Alliance, their new technology CSR5, offers a cost-effective solution to implement a best-in-class cybersecurity program that has three main components: 1) Software – Defense; 2) Cyber Education; and 3) Oversight.

This program reduces overall risk, implementation, costs, knowledge, and improves resiliency, strategically positioning businesses for response and recovery. If you become a paid member of CSGA you can now participate in the journey which will create the future of cybersecurity and cyber defense today.



Our people are what make CSR5 Security Software unique. Cyber Security Global Alliance (CSGA), provides our security solutions with patent ready collaborative solutions in an AI-driven environment that supports professional and economic growth.

Our executive teams of CSGA and CSR5 give our strategic partners and staff a voice. Our teams are put together with the help of our human resources management team to ensure that we receive maximum productivity and commitment from the people within our organization.

CSR5 provides tailored products and services to its members, including risk reduction of initial cyber breaches and professional assistance in defending against active threats. Plus, each member company gains access to our 24/7 hotline. Our team will assess the unique situation, advise on immediate next steps, and connect each member to the appropriate vetted and capable solution providers on a case-by-case basis.

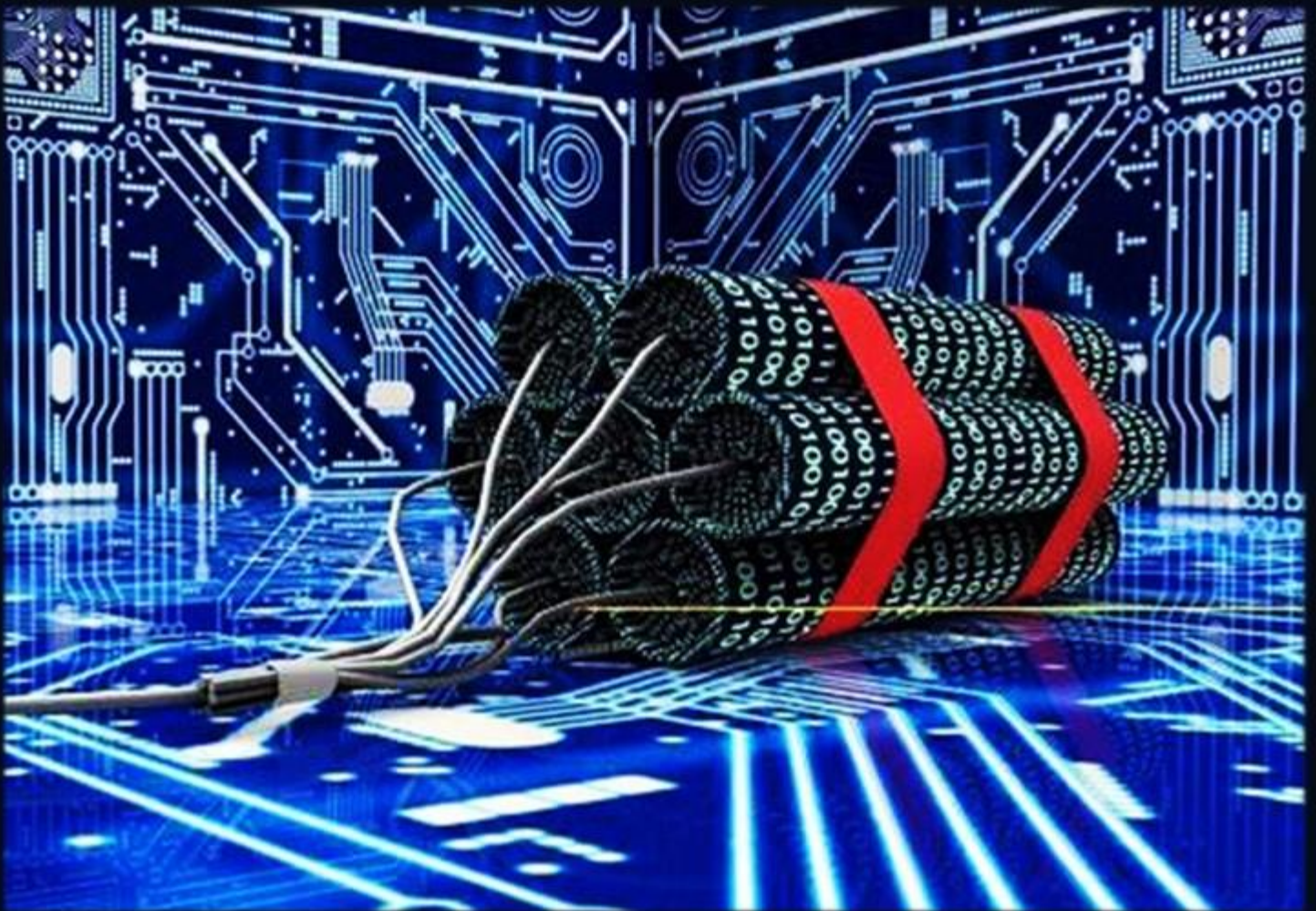


JAMES CASTLE

CHAMPIONING CHANGE

Cyber Threat and Criminal Organizations Through Cyber Terrorism

Cyberterrorism is defined by the U.S. Federal Bureau of Investigation as a premeditated attack against a computer system, computer data, programs, and other information with the sole aim of violence against clandestine agents and sub-national groups. The main aim behind cyberterrorism is to cause harm and destruction.



Some of the direct effects of cyberterrorism can include ransomware and malicious attacks, which could potentially lead to acts of extremism and terrorism through political unrest and community disfunction. This can lead to deeper issues such as cyberwarfare and cyberattacks against critical infrastructure.

Worst case scenarios can lead to committing severe, nation-wide attacks against our global defenses, this is also known as a national fire sale, which is designed by threat actors to compromise our national secrets and security, putting these assets up for sale to the top buyer. The extension of these types of attacks could upgrade to Quantum AI threats or worse. If Quantum was used with artificial intelligence, then the threat of global terrorism could potentially lead to terrorist threats of global thermonuclear war using a state-of-the-art quantum tech that could not be stopped making the threat real.

If threat actors could bypass our toughest security platforms, holding the world ransom with the potential threat of nuclear war is possible. Anyone could do this. A threat actor can be a common computer hacker or be a community leader, or even the leader of a country. The safeguards till now have not been possible, governments do not see the bigger picture, people think the governments control the situation and yet everyone doesn't realize the potential threats that can be caused by Quantum AI.

That is until James Castle came to the cyber sector with a vision to stop cyber threat altogether, finding the real solutions for these problems. It is time for people to wake up and pay attention to the true threat, Quantum AI.

Here are some pointers that we as humanity must come to grip with:

- Most people underestimate the threats around us.
- In Canada, our federal government is thoroughly confused and will get buried by various Bill's (for example Bill C-27 in Canada) will very quickly become very Orwellian, as there is already significant censorship online today). These acts play directly into the hands of the black hats.
- Many people are unaware of what quantum technology is, the threats it poses, and the potential damage it can cause, including the varying levels of severity between quantum technology and artificial intelligence.

In the Western world today, only one group has quietly solved the critical problem of cyber threats using blockchain security and quantum through software - **CSR5 Global Threat Response Software.**

Fully downloadable, controllable, and customizable, James Castle and his global

team of cyber defense experts and scientists at Cyber Security Global Alliance have perfected this technology, which was unveiled at Canada's premier IT and Cyber Trade Show, the "iTECH Conference."

On November 19, 2024, James Castle delivered a compelling presentation titled "The Pros and Cons of Quantum Security" to a full room of intrigued individuals and organizations at the event in Toronto.

In today's movies, we often see stories about robots and advanced technologies taking over the world, fueled by themes of terrorism and the wars sparked by artificial intelligence. For example, the original *Terminator* films explored the concept of a quantum chip driving these catastrophic events.

Quantum Warfare is the thing that people need to be aware of, the true threat, far worse than the threat of AI, additionally identified by James Castle (AI2) as the clarity between artificial and augmented intelligence and how it is being applied today.

Humankind has long marvelled at its digital achievements, but where do we draw the line in our technological progress when the world struggles to fully understand these advancements and their potential negative consequences, especially when in the hands of a threat actor or terrorist? A clear definition of this is essential, particularly in the context of ransomware's impact and how such attacks are reported to the government.

Recent statistics from the Canadian government show that ransomware has caused nearly \$10 trillion USD in damages over the past two years.

Despite the government's efforts to create legislation and compliance measures to address this threat, cybercriminals continue to stay ahead. The solution does not lie in more legislation, compliance, or AI - it lies in directly solving the problem.

As of November 19, 2024, that solution has been found.

Over the next decade, government bodies will attempt to drive progress with promises of unbiased political support. However, this is challenging, as governments are limited by their term lengths. When leadership changes, progress can be stalled and set back to square one. Even reverse engineering is not an option, as the technology itself is secure and cannot be hacked. The true proof of concept lies in the functioning technology, which will naturally attract people, investment, and opportunities as it continues to prove its value.


Who would you entrust to make sure this technology remains secure? Who should regulate the decision of how laws reflect data protection? Which country should have that right above all else? In my opinion there is only one organization with that right, and it is the body of people and organizations that created that solution alone and that is a Canadian non-profit, a membership-based, non-governmental organization called Cyber Security Global Alliance or CSGA, which holds the future of quantum security and will regulate its safety globally.

The key building blocks for quantum security rely on:

1. Effective Cross-Border Legislation (To Be Determined)
2. Cybersecurity Maturity Model Certification Compliance (U.S. DoD and Cyber AB)
3. National Supply Chain Security Program (Outside the USA) developed by Terranova Defense USA
4. Global Oversight Board and Center of Excellence (CSGA Membership)
5. Standard of Care (CSGA Members Elected Policies)
6. Cross-Border Cyber Rules (Enforced by law enforcement)
7. Global Lobbying Body for Cybersecurity Law Creation
8. Shared Information for NATO Approved Countries
9. Proper Non-Bias NATO ATS Security Clearance Checks for All Providers and Salespeople
10. Cyber Intelligence Division (Already Developed and Operational)
11. Global Certification Body (U.S. 501C3 - Foundation) Already Operation

These key building blocks have been developed and are now in place, creating the global framework required to shift the world's mindset and address the root causes of the global cyber threat.





Cyber threats today are spiralling out of control. This threat cannot be managed or enforced through conventional means, but it can be stopped. Not by legislation, not by enforcement, and not by brute force.

Cyber threats can only be neutralized through advancing technology - and that technology has already been created by a Canadian non-profit (CSGA) and its corporate partners. Together, since 2021, we have been empowering small businesses to collaborate and strengthen the economy through mutual commitment to change.

Our operations are based in the North's Silicon Valley, Kitchener, Ontario, Canada, with our partners and corporate board members spanning 21 countries worldwide. The world is in dire need of change. Our economy needs saving, and we must unite behind a common cause. As the world's cyber champion and visionary, James Castle has taken a stand to help humanity overcome the cyber threat obstacles we face, and his team stands by his side and together we will change the world and stop global cyber threat once and for all.

*~ **James Castle**, Chief Executive Officer & Founder*

@ Terranova Aerospace and Defense Group Corporation

terranova-secdef.com

& Executive Director and Founder

@ Cyber Security Global Alliance (CSGA)

CSH

@thecybersecurityhub



The **Cyber Security Hub™**

@thecybersecurityhub

World's Premier Cyber Security Portal

Four Cyber Experts *for* Breaking Cybersecurity Stereotypes



Stereotypes surrounding STEM fields often deter young women from exploring careers in cybersecurity, perpetuating gender disparities. These biases can extend to hiring practices, limiting opportunities for highly qualified female candidates.

~ **Anurag Chandra**, West Delhi, India



Cybersecurity is a collective responsibility that impacts every level of the organization. By fostering awareness and promoting a proactive, collaborative approach, we can create a resilient digital environment where every employee becomes a key defender against cyber threats.

~ **Dorothee Decrop**, Paris, France



Albania is breaking barriers in cybersecurity, challenging stereotypes with bold initiatives. By addressing systemic barriers and fostering diverse participation, the country is laying the groundwork for a cybersecurity ecosystem that is both innovative and resilient.

~ **Esmeralda Kazia**, Tirana, Albania



Cybersecurity often exists in the shadow of misconceptions - myths that paint an inaccurate picture of the industry and deter potential talent. ...It is critical to break down these barriers and present a clearer, more inclusive perspective of what cybersecurity truly entails.

~ **Wojciech Ciemski**, Warsaw, Poland

Redefining Cybersecurity by Breaking Barriers From Bias to Brilliance

by Anurag Chandra, CRISC, CISA, CISM... , India

*“Cybersecurity is not just an IT issue but a **collective responsibility** that impacts every level of the organization. By fostering awareness and promoting a proactive, collaborative approach, we can create a resilient digital environment where every employee becomes a key defender against cyber threats.”*

~ Dorothee Decrop,
the Déléguée Générale (equivalent to General Director) of Hexatrust, France

Breaking Stereotypes in Cybersecurity: A Call for Inclusivity

STEM Education standing for Science, Technology, Engineering, and Mathematics being an interdisciplinary approach to learning where academic concepts are coupled with real-world lessons. This enables the literacy development making young generation to compete in this new economy.

Stereotypes surrounding STEM fields often deter young women from exploring careers in cybersecurity, perpetuating gender disparities. These biases can extend to hiring practices, limiting opportunities for highly qualified female candidates.

Interestingly, while such biases were earlier more pronounced in developed countries, they appear less prevalent now in few regions of Asia, particularly in India, where a growing emphasis on inclusivity is breaking traditional barriers in this era of Digital India program; **Vikassheel to Viksit Bharat 2047** emphasising Security, Trade and Technology.

In many traditional Asian rural families, the **mindset** persisted that a girl over the age of 18 should prioritise marriage over career and learning. This **cultural expectation** often overshadows the potential for young women to pursue careers in fields like cybersecurity. Additionally, **societal norms** have historically dictated that activities such as gaming and drone technology are for boys, while girls are expected to engage in cooking or playing with Barbie dolls and kitchen sets rather than plying in the field. This **gendered division of interests** further discourages girls from exploring technology-related fields.

Young women pursuing STEM careers face several significant challenges that can hinder their progress and in turns National progress while discouraging them from continuing in these fields. Some of the key barriers:

- **Gender Bias and Stereotypes:** From a young age, girls often encounter stereotypes that suggest they are less capable in math and science compared to boys. These biases can be reinforced by teachers, peers, and even family members, leading to a lack of confidence and interest in STEM subjects.
- **Workplace Culture:** Women in STEM careers often face exclusionary cultures and environments that are predominantly male. This can lead to feelings of isolation and being undervalued.
- **Wage Gap:** Women in STEM fields often earn less than their male counterparts, even when they have similar qualifications and experience.
- **Balancing Family and Career:** Many women face the challenge of balancing family responsibilities with demanding STEM careers. This can be particularly difficult in fields that require long hours or frequent travel.
- **Educational Barriers of Digital Divide:** Access to quality STEM education might be limited, especially in rural or underprivileged areas. Girls in these regions may not have the same opportunities to engage with STEM subjects as their urban counterparts.

However, the **landscape is gradually changing**. In today's multinational era of learning, it is **imperative to challenge** and change these cultural mindsets.

Despite the progress, rural India still faces significant challenges. **Honour killings**, driven by caste-based marriage expectations, continue to overshadow the importance of education and career growth for young women.

*To truly break these stereotypes, we must **foster an environment** where girls are encouraged to explore and excel in cybersecurity and other STEM fields.*

This involves not only changing societal attitudes but also implementing policies that support gender inclusivity in education and the workforce. Therefore, **promoting STEM education** for girls from a young age is crucial for several many reasons:

- **Bridging the Gender Gap:** Young women who are good in coding and wanting to pursue their career in emerging technologies can be encouraged rather than getting stuck to the traditional mindset of STEM fields being male dominated. By encouraging girls to engage with STEM subjects early, we can start to balance the gender disparity.
- **Empowering Future Leaders:** Education should be encouraging education and learning without any gender biasing that equips young boys and girls together with critical thinking, problem-solving, and analytical skills. These are essential for leadership roles in any field. Example Programs like the National Center for Women & Information Technology (NCWIT) offer resources and support to help young women succeed in tech careers.

- **Economic Benefits:** STEM careers are among the fastest-growing and highest-paying jobs. Encouraging girls to pursue these fields can lead to greater economic independence and stability. For instance, women in STEM jobs earn 33% more than those in non-STEM occupations.
- **Innovation and Diversity:** Diverse teams are more innovative and effective. By bringing more women into STEM, we can foster a broader range of ideas and solutions.
- **Supportive policies:** The newly married or the young mothers could get the support of flexible working hours and parental leave, which might be essential to help women manage these traditional tabooed responsibilities.

Also, by showcasing successful female role models in cybersecurity - women who exemplify the impact and leadership they bring to this critical field - and promoting STEM education for girls from an early age, we can start to dismantle the barriers that have long hindered gender equality in these areas. Highlighting outstanding achievements would hopefully inspire more young women to consider pursuing careers in this dynamic and essential industry.

In my **concluding remarks**, I would like to emphasise that the cybersecurity field is often clouded by stereotypes that deter young women from pursuing careers, perpetuating gender disparities.

These biases, especially prevalent in developed countries, limit opportunities for talented female candidates. However, regions like India are making strides towards inclusivity, breaking down traditional barriers.

Despite this progress, rural areas still grapple with cultural challenges, such as prioritizing marriage over education for young women and gendered expectations around technology.

To dismantle these barriers, we must create an environment that encourages girls to explore and excel in cybersecurity from a young age.

By showcasing successful female role models and implementing supportive policies, we can enrich the field with diverse perspectives, drive innovation, and pave the way for a more inclusive future.

Anurag Chandra, India

Experienced CISO | Cybersecurity & Digital Transformation Leader

Anurag Chandra is a distinguished technology and cybersecurity leader with over 25 years of expertise in the Defence and Aviation sectors. His career has been defined by a deep focus on IT strategy, security, and risk management, coupled with a passion for tackling complex challenges.

As a seasoned Chief Information Security Officer (CISO), Anurag has consistently delivered future-ready security strategies, streamlining workflows, and enhancing operational efficiency. His innovative leadership and strong program management skills have made him a trusted figure in risk mitigation, compliance, and organizational transformation.

Areas of Expertise

- IT Strategy and Security
- Artificial Intelligence and Cybersecurity
- Cyberpsychology and Digital Forensics

Education

- Master of Technology in Quality Management – Birla Institute of Technology and Science, Pilani
- Master of Business Administration in International Business – Indian Institute of Foreign Trade
- Bachelor of Engineering in Computer Science – North Maharashtra University

Certifications

- ISO 42001
- Certified Cyber Crime Investigation Officer
- CRISC, CISA, CISM, and PMP
- Various Cloud Technology Credentials



Diversity as a Catalyst for Cybersecurity

Albania's Leadership in Inclusion and Innovation

by **Esmeralda Kazia**, Tirana, Albania

Cybersecurity can be likened to a complex mosaic, where each unique piece contributes to a resilient and innovative system. In Albania, women are emerging as key contributors to this intricate structure, redefining traditional roles and advancing the field with inclusion and creativity. Their leadership is not only transforming the national narrative but also serving as a critical element in building a more adaptive and robust cybersecurity framework.

Albania is breaking barriers in cybersecurity, challenging stereotypes with bold initiatives. Its active engagement in programs such as the European Cybersecurity Challenge (ECSC) underscores its commitment to redefining the field. These competitions provide an international stage for young Albanian talents, fostering collaboration and skill development while challenging the perception of cybersecurity as a male-dominated discipline. Through these efforts, Albania is cultivating a culture where diversity is celebrated as a strength.

Women, who have historically faced underrepresentation in technology, are now at the forefront of Albania's cybersecurity landscape. Their participation is supported by mentorship programs, leadership development initiatives, and public awareness campaigns aimed at reshaping societal perceptions. These movements are empowering women not only to contribute but also to lead, inspiring a new generation to view cybersecurity as an inclusive domain.

These advancements align with Albania's national cybersecurity strategy, which emphasizes inclusivity, education, and international cooperation. *By addressing systemic barriers and fostering diverse participation, the country is laying the groundwork for a cybersecurity ecosystem that is both innovative and resilient.* This strategy reflects Albania's broader vision of turning challenges into opportunities, leveraging the power of diversity to drive progress.

Albania's efforts illustrate that the future of cybersecurity is inherently collaborative and inclusive. By integrating diverse perspectives, the country is creating a dynamic and sustainable foundation for global innovation, proving that every voice matters in securing our interconnected world.



Esmeralda Kazia, Tirana, Albania, serves as the ***Director of Monitoring and Incident Response, Operations Center SOC, C-SIRT*** within Albania's National Cyber Security Authority (NCSA). With over a decade of experience in cybersecurity and IT, she leads efforts to safeguard critical infrastructure against evolving threats.

Holding a Master's in Computer Engineering from Fatih University, her expertise spans data security, data science, and advanced IT strategies. An accomplished academic and thought leader, Esmeralda has spearheaded major initiatives, contributed to groundbreaking research, and shaped national cybersecurity strategies.

Currently pursuing doctoral studies, she remains at the forefront of innovation and resilience in the digital age.

Breaking Cybersecurity Stereotypes

Redefining the IT Security Industry

by **Wojciech Ciemski**, Poland



The field of cybersecurity often exists in the shadow of misconceptions - myths that paint an inaccurate picture of the industry and deter potential talent. Whether it's the image of the lone genius typing away in solitude or the exclusive association of cybersecurity with "hacking," these stereotypes do more harm than good. For the industry to thrive and evolve, it's critical to break down these barriers and present a clearer, more inclusive perspective of what cybersecurity truly entails.

Cybersecurity: A Team Sport, Not a Solo Mission

The popular image of a lone genius working in isolation to crack impossible codes is a myth deeply rooted in pop culture. While it may make for an entertaining movie plot, the reality is far more collaborative. Modern cybersecurity demands teamwork across various disciplines. From analysts and developers to network administrators and communication specialists, every role plays a crucial part in safeguarding systems.

Take incident response as an example. This process requires seamless coordination: one team detects anomalies, another investigates the threat, while yet another devises remediation plans and communicates the situation to stakeholders. Without a cohesive team, the effort falls apart.

In cybersecurity, the myth of the lone wolf solving problems in isolation is not only inaccurate, it is damaging. It overlooks the importance of diverse expertise and teamwork in addressing increasingly complex threats.

Diversity in Cybersecurity: Busting the 'tech bro' myth

Dominating the Cybersecurity field has been the stereotype of a tech savvy male in the youth culture, a hoodie wearing x and y. But this is bound to change as class and sex discrimination still exists within the field.

Women considered as a minority in tech communities have now grown to 25% in Cybersecurity field and that percentage is growing. There is also a shift towards women joining the workforce and this is not just a shift in sex but in how problems will be approached and looked at.

Through experiences, culture, and thought diversity that include various aspects outside the box allows teams to be able to address problems, anticipate threats and create solutions that respond to global users.

In addition, Companies are starting to realize the importance of diversity and that having one stream is not effective. Threat actors come from every corner of the world, and a varied team tackling global challenges is more effective. The Cyber Security field doesn't only have this tech bro stereotype but has the potential which this stereotype undermines.

Cybersecurity isn't just about hacking

Cybersecurity is commonly associated with an image of a hacker, usually a person behind a terminal with lines of text scrolling across the screen, so the first association is quite normal. However, this is just one aspect of the issue. Cybersecurity is a broad discipline that integrates risk, compliance, education, and engineering, among others.

Take risk management for instance where specialists assess the risk and then implement actions aimed at engineering those risks down. Legal professionals, however, work against such risks, helping the organizations comply with regulations such as the General Data Protection Regulation or the Network and Information Security Directive 2, in order to enhance data and non-financial assets dissipation. Equally important, however, is the role of educators, who help people learn to identify phishing attempts or simply educating how to keep devices secure.

Even in technical positions, not everyone is a penetration tester or a vulnerability researcher, as such positions are based on the weakest link in any complex system. Security engineers center around building useful systems whereas analysts concentrate on finding and responding to threats. The variety of roles means that not everyone in cybersecurity is expected to be a hacker but rather have the motivation to make a difference and create.

Cybersecurity isn't a boys' club anymore

The relative scarcity of women in the cybersecurity sector is gradually changing as more women are taking up leadership positions. However, such transformation does not occur organically, but it takes a joint effort by companies as well as industry players to enable the changes.

Mentoring is perhaps the most active forms of furthering actions towards equity. The older members of the industry can assist those entering the field, particularly in younger professionals from under-represented populations, in addressing specific realities practitioners face. Equally important is the need to conduct impartial selection procedures and put

in place active efforts to increase the number of such role models. Representation is significant not only to enable today's youth envision their future careers, but also several across the ecosystem so that the industry is inclusive for everyone.

The myth of perfect defence

The biggest common misconception in IT security is that a hacker will not find his way into a properly secured system. Unfortunately, this is not the case and no system can be considered perfect. It is not enough to undertake one effort and intend it to be the end, an organisation has to continuously monitor and improve the security of its systems.

Systems are prone to human error, zero-day vulnerabilities, and continuous evolution of attack vectors. The aim here is not to become flawless but rather to withstand threats. Some of the measures which fall under this category would include installation of robust prevention measures, routine vulnerability checks and team engagements to risk lower the probability of risks.

The fact that this is the case is self-affirming. It changes the story from an unrealistic expectation of never being breached, to an achievable objective which is growth in the future.

Breaking down barriers to entry: Cybersecurity isn't just for experts.

The myth that cyber security is the preserve of experts, is one of the most worrisome generalizations. In reality, the possibility is open to any person who strives to acquire such knowledge. One does not need a diploma in computer engineering or numerous years of hands-on technical skills to begin. Fundamental concepts are also provided in some of the online classes.

For starters, Wireshark or Nmap are basic tools that can be used effectively. A variety of skills and interests may then be showcased during the development of a portfolio based on individual work or attendance at hackathons. Cyber Security is not an exclusive domain but one that is college of the interested and the willing.

How IT professionals can help break stereotypes

You are an IT specialist. You belong to the group that has the most potential to change the narrative of cyber security. You can practice what you believe and, therefore, break the stereotypes.

Make it your first point to foster your workplace's diversity. Support diverse role models within Cybersecurity. Educate people by sharing blogs, creating webinars, and having conversations with interested people. Most importantly, be a role model – don't just state that it's all about technical skills, but rather creativity, cooperation, and lifelong education as well.

Conclusion: A call to action for IT professionals

Destroying the existing stereotypes around the industry of cybersecurity is not only important for the branding of the industry – it is needed for its sustainability. A more representative and holistic focus in approaches to security will promote a greater diversity of skills– and in the end be better for the profession.

It is our responsibility as professional to address these issues and build a very specific vertical that isn't too plain and unimaginative like how the world it strives to protect appears. Cybersecurity is for everyone – it is about time for the world to see it this way.





Wojciech Ciemski, with over a decade of experience, serves as a **vCISO** and is a laureate of the “40 under 40 in Cybersecurity 2024”. He authored the bestselling book “Cybersecurity in Questions and Answers” and founded **Security Bez Tabu®**, one of Poland's top cybersecurity blogs.

A sought-after speaker at major conferences like **SEMAFOR**, **OhMyH@CK**, and **The Hack Summit**, Wojciech has trained over 2,000 people in more than 500 hours of live sessions. His practical expertise and dedication to educating the next generation make him a key figure shaping the future of cybersecurity.

**“I Always
Repeat**



**Read, Read,
Read!”**

Nadine Gordimer
Nobel Prize in Literature, 1991

Human Rights and Their Controversy in the New International Convention Against Cybercrime

by **Claudia Bonard de Carvalho**, Brazil

Recently, the UN in New York approved the draft of a new treaty on cybercrimes, known as the Convention against the Use of New Technologies for Criminal Purposes¹. This convention regulates issues from the previous Budapest Convention, now focusing on detailing international cooperation in combating cybercrime.

The text of the proposal is fundamentally based on respect for the domestic legislation of each country and the adoption of international cooperation measures, given the many obstacles raised by the signatories of the Budapest Convention, which remains in effect, as well as on the protection of critical infrastructures, such as energy and transportation services, which have been heavily targeted by cybercriminals.

Critics of the new treaty argue that the proposal could be a blank check for attacks on human rights, but several considerations must be made:

1. The argument that the convention could facilitate human rights violations is weak because such violations could occur even if the treaty did not exist, simply through the application of the laws of each signatory country on the treaty's topics, and the text of the convention itself contains an explicit commitment to their protection².

2. The text states that privacy rights must be respected during investigations³; which solely depends on the signatories' efforts to adopt a data protection law regulating public security, which should already exist independently of the convention.

3. The convention also addresses issues of extraditing suspects, which is a matter of international law and is equally subject to each country's regulations on the matter.

4. Critics also argue that there could be over-surveillance of citizens due to the potential sharing of electronic evidence in cooperation between countries, despite the fact that efficient combat against cybercrime is impossible without international cooperation. Cybercriminal gangs' activities evolve constantly to continue attacking businesses and public institutions, making it unrealistic and ineffective to avoid such cooperation, as demonstrated by the success of various police operations in capturing members of groups like Revil, Lockbit, etc.

1. Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Disponível em: <https://www.scientificamerican.com/article/0724--un-cybercrime/>. Acesso em 22.08.24.

2. Article 5. Respect for human rights States Parties shall ensure that the implementation of their obligations under this Convention is with their obligations under international human rights.

3. Article 36. Protection of personal data - States Parties shall not be required to transfer personal data in accordance with this Convention if it cannot be provided in compliance with their applicable laws concerning the protection of personal data.

5. Regarding the alleged violation of citizens' privacy in police investigations, national laws already set limits on authorities' actions when requesting access to providers' data. In Brazil, for instance, the Internet Framework (Law No. 12.965/14)⁴ mandates that police requests must be justified according to its principles, under penalty of being abusive. If such laws do not exist in a signatory country, the International Convention on Human Rights and the Citizen must still be respected.

6. The treaty in question includes various human rights safeguards, which were even contested by some countries involved in drafting the convention's text for being excessive⁵. It is important to remember that treaties do not have the power to interfere with the sovereignty of each country, whose respect was expressly highlighted in the draft⁶. This is a sensitive issue in international law to avoid unnecessary clashes between governments in a world where several armed conflicts are still ongoing.

Thus, although the convention presents questionable points, it represents an important step towards the global commitment to combating cybercrime.

- 4. Art. 10. The retention and availability of connection records and internet application access records referred to in this Law, as well as personal data and the content of private communications, must respect the preservation of the privacy, private life, honor, and image of the parties directly or indirectly involved.
- 5. Disponível em: https://www.lemonde.fr/en/pixels/article/2024/08/09/un-approves-its-first-treaty-targeting-cybercrime_6711661_13.html. Acesso em 22.08.24.
- 6. Article 4. Protection of Sovereignty - 1. States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States.





Claudia Bonard de Carvalho, Brazil

Recognized as one of the Top Women in Cybersecurity LATAM by WOMCY - Women in Cybersecurity, Claudia Bonard de Carvalho is a criminal lawyer in Rio de Janeiro. Graduated from the State University of Rio de Janeiro and trained in cyber risk management at FGV-SP, Claudia is specializing in corporate cybercrime.

Claudia's distinction spans the continent, and her additional roles include Professor of Cybercriminology at the Future Law course; columnist for the CyberTechBrasil Movement; author of the book *Direito Penal 4.0*; mentor in cybercrime at AB2L (Brazilian Association of Legal Techs)...



Navigating Global AI Governance

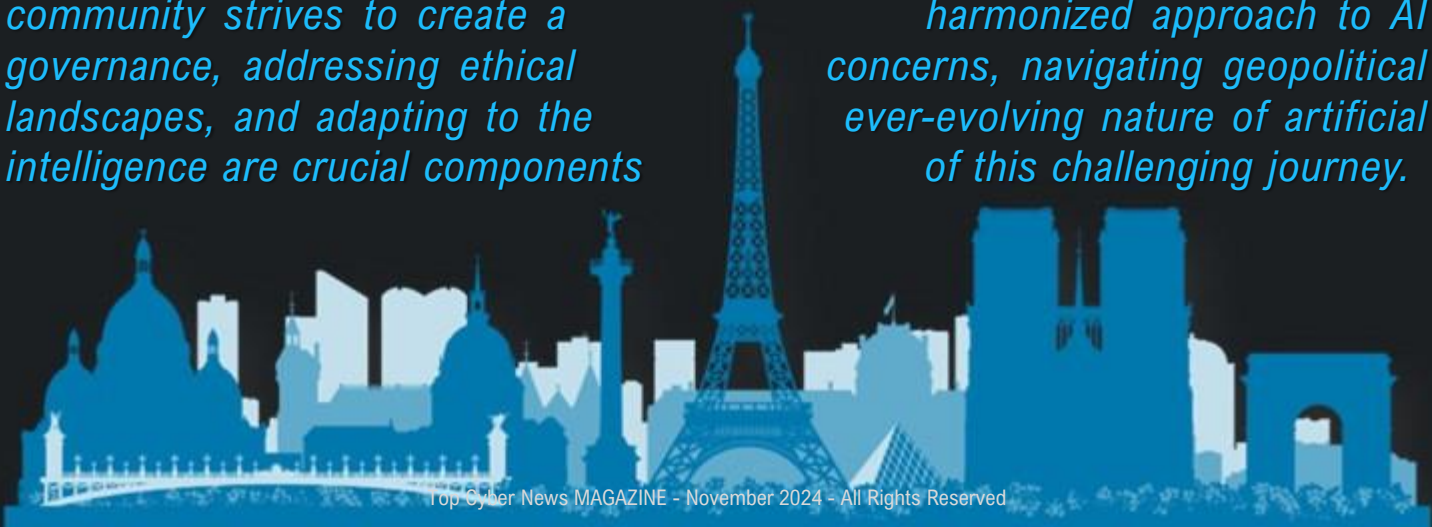
by **Alexa Charles**, France

The surge in initiatives to regulate artificial intelligence (AI) has prompted the question of who will take the lead in governing this rapidly advancing technology. *Europe is at the forefront with the AI Act, aiming to establish an international framework for AI regulation.*

A comprehensive approach to AI governance is essential, balancing regulation with the desire for innovation. Addressing the complexity of certain AI systems, particularly generative models, poses a challenge. The depth of these models' foundations makes it difficult to understand their inner workings, raising questions about accountability and transparency. Explainability and traceability become crucial considerations, especially with generative AI. As the technology evolves rapidly, navigating its accelerating complexity is paramount, particularly when dealing with systems that generate outputs beyond full comprehension.

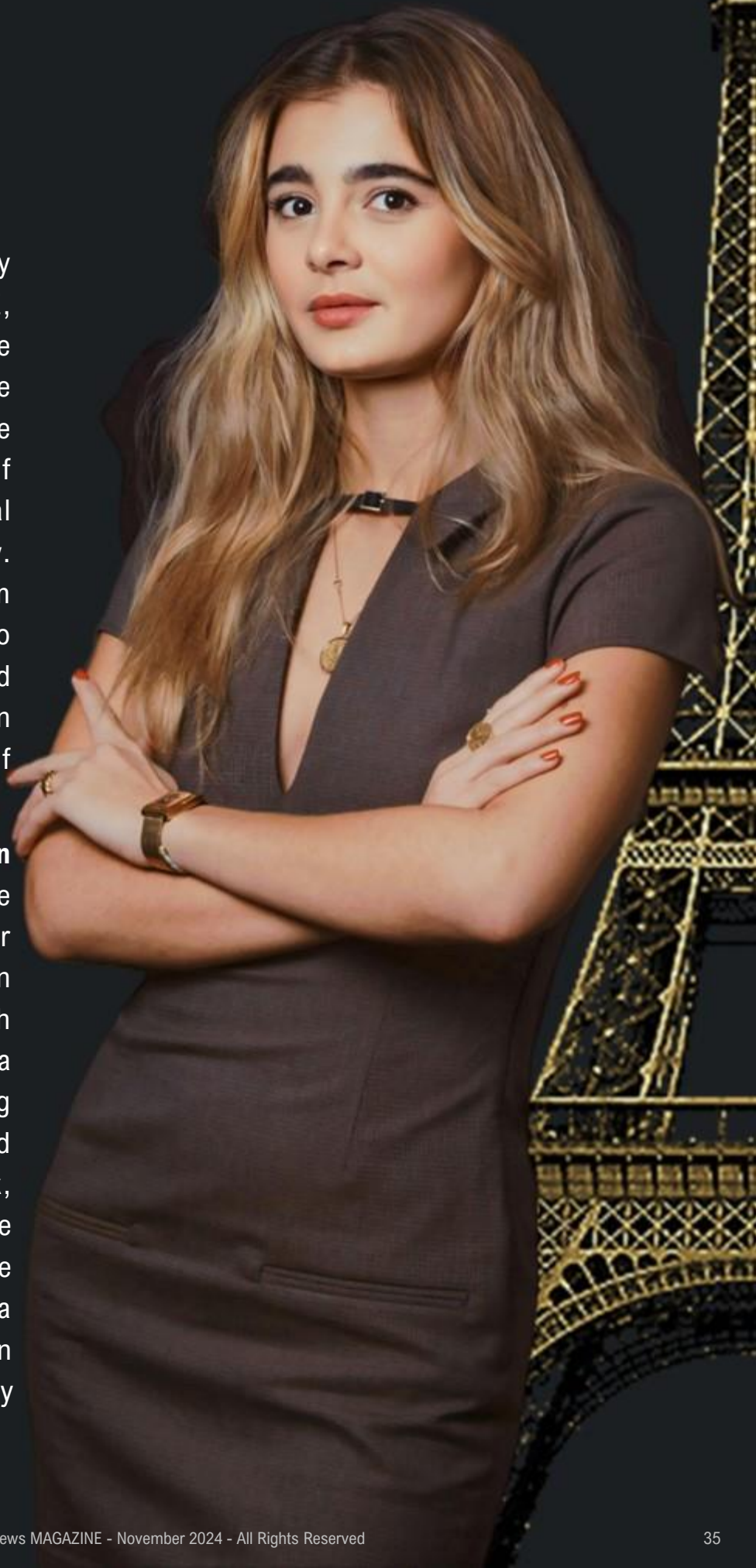
The protection of personal data in the context of AI is also an important issue. In Europe, the GDPR is the European regulation in application since 2018 and impacts all companies operating personal data processing. *This is a crucial issue in the governance of AI, in terms of how datasets can be used, especially as not all countries have the same regulations in terms of personal data protection.* While data minimization is important, it does not necessarily restrict training AI systems on large datasets. Existing governance models in the United Kingdom, the United States and Europe could serve as a foundation for a global governance framework. However, achieving global collaboration on AI governance requires ethical consensus and acknowledgment of national and geopolitical interests.

In conclusion, *the governance of AI demands a delicate balance between regulation and innovation, transparency and complexity. As the international community strives to create a harmonized approach to AI governance, addressing ethical concerns, navigating geopolitical landscapes, and adapting to the ever-evolving nature of artificial intelligence are crucial components of this challenging journey.*



40 under 40 in Cybersecurity by Top Cyber News MAGAZINE, **Alexa Charles** serves as the **Program Manager** of the **InCyber Forum** and is the **Editor-in-Chief** of "**CyberLeaders**", an annual strategic cybersecurity review. In her role as the Program Manager, she is empowered to cultivate collaboration and share valuable insights within the ever-evolving realm of digital security.

Holding a **Master's degree in Criminology** from the **Université de Montréal**, her thesis delved into information sharing in Cybersecurity. With two years of experience as a **Senior Analyst** in fighting against money laundering and terrorism for a **Canadian bank**, Alexa is now a passionate advocate for fostering knowledge exchange and promoting a more secure digital world within the worldwide cybersecurity community.



The Rise of Algorithmic Auditing

Preparing Cybersecurity Executives for AI Regulation

by **Akhil Mittal, CISSP, CCSP**, United States

“Algorithmic auditing refers to the process of evaluating the functionality of machine learning (ML) applications, including the context and purpose of the machine to assess utility and fairness.”¹

~Varun Prasad, CISA, CISM, CCSK, CIPM, PMP

Artificial intelligence (AI) is reshaping industries like finance, healthcare, and cybersecurity, driving efficiency, automation, and informed decision-making. But as businesses increasingly rely on AI, ensuring that these systems are secure, fair, and explainable has become a critical issue - particularly for cybersecurity executives. With regulations like the **EU's AI Act** gaining momentum, algorithmic auditing has quickly emerged as a crucial practice to ensure AI systems are transparent, compliant, and protected against misuse or exploitation.

AI Compliance: An Urgent Priority for Cybersecurity Teams

One of my clients recently launched an AI-driven fraud detection model that significantly improved their ability to detect fraudulent activity. The team was excited by the results - until the legal team raised a critical question: *Can we explain how this model is making its decisions?* Excitement quickly turned into concern. Was the model fair? Could it be biased? Most importantly, could they justify its decisions to regulators? These weren't just hypothetical concerns - AI regulation was looming, and answers were needed.

Cybersecurity teams are used to protect data, but AI introduces new layers of complexity. As regulations, particularly in the EU, push for transparency, fairness, and accountability, cybersecurity leaders must adapt to stricter standards.

This is where algorithmic auditing comes into play - it ensures AI models meet these standards while staying secure against emerging threats.

Why Algorithmic Auditing is Critical

AI models, especially those powered by complex machine learning algorithms, often operate as “black boxes” - making decisions that even their creators struggle to explain. This lack of transparency poses significant risks, particularly in industries where accountability and precision are essential. Governments are responding to these risks by rolling out regulations like the EU's AI Act, which require transparency and accountability for high-risk AI systems.

-
1. Prasad, V. (2024, August 2). *AI algorithm audits: Key control considerations.*
<https://www.isaca.org/resources/news-and-trends/industry-news/2024/ai-algorithm-audits-key-control-considerations>

Algorithmic auditing - the systematic evaluation of AI models - helps businesses ensure their AI systems are fair, compliant, and secure. In my experience, organizations that fail to audit their AI systems risk reputational damage, legal challenges, and significant financial penalties.

Key Risks to Watch

AI brings unique security challenges that traditional IT systems don't encounter. Two key risks to watch include:

Data Poisoning: Adversaries inject manipulated data into an AI model's training set, leading to biased or inaccurate results. To prevent this, cybersecurity teams must secure data pipelines and monitor unusual data patterns in real time

Model Extraction: Attackers repeatedly query an AI model to replicate its functionality, potentially exposing its underlying logic. Limiting query access and applying differential privacy techniques can obscure how the model operates, making it more difficult for adversaries to replicate the model.

Steps for Cybersecurity Teams to Prepare

1. Foster Cross-Functional Collaboration

A common challenge I see is the disconnect between cybersecurity, data science, and legal teams. AI models, with their technical complexity, are often developed in silos without enough input from security or compliance experts. This fragmented approach can lead to models that are opaque or non-compliant.

To make algorithmic auditing effective, collaboration between these teams is essential. Involving cybersecurity early in the AI development process allows organizations to identify risks before deployment, ensuring that models are transparent, secure, and compliant from the start.

2. Implement AI Governance and Automate Audits

Given the complexity of AI models, a robust AI governance framework is essential. This framework should continuously monitor AI systems for compliance, fairness, and security. Automating audits provide real-time insights, flagging potential biases or discrepancies as they arise.

By automating the auditing process, organizations can manage the large volume of AI models they deploy more effectively, ensuring compliance and transparency at scale.

3. Conduct Regular Adversarial Testing

Just as regular audits and penetration tests are standard practice in traditional cybersecurity, AI models require adversarial testing to uncover vulnerabilities. This involves probing AI systems with inputs designed to manipulate their outputs, revealing weaknesses that attackers could exploit.

For instance, adversarial testing of one client's AI-driven threat detection system revealed that it was ignoring certain types of malware - exposing a critical security gap that might have otherwise gone unnoticed. Regular adversarial testing helps prevent such vulnerabilities from becoming serious issues.

4. Monitor Global Regulatory Trends

AI regulation is evolving rapidly. The EU's AI Act is setting the global standard for AI governance, but U.S. regulators like the Federal Trade Commission (FTC) are also advancing their efforts. To stay ahead of these changes, cybersecurity teams must establish internal processes to continuously monitor and adapt to new regulations.

A dedicated task force focused on tracking regulatory developments can help ensure your organization remains compliant as laws evolve, especially as more countries begin to adopt AI-specific regulations.

Overcoming AI Auditing Challenges

Proactively Addressing AI Risks

There's a common misconception that algorithmic auditing is only necessary for large enterprises with complex AI infrastructures. In reality, even small and mid-sized organizations can implement scalable auditing practices using open-source tools. These solutions make it easier for businesses of any size to ensure their AI models meet ethical and regulatory standards.

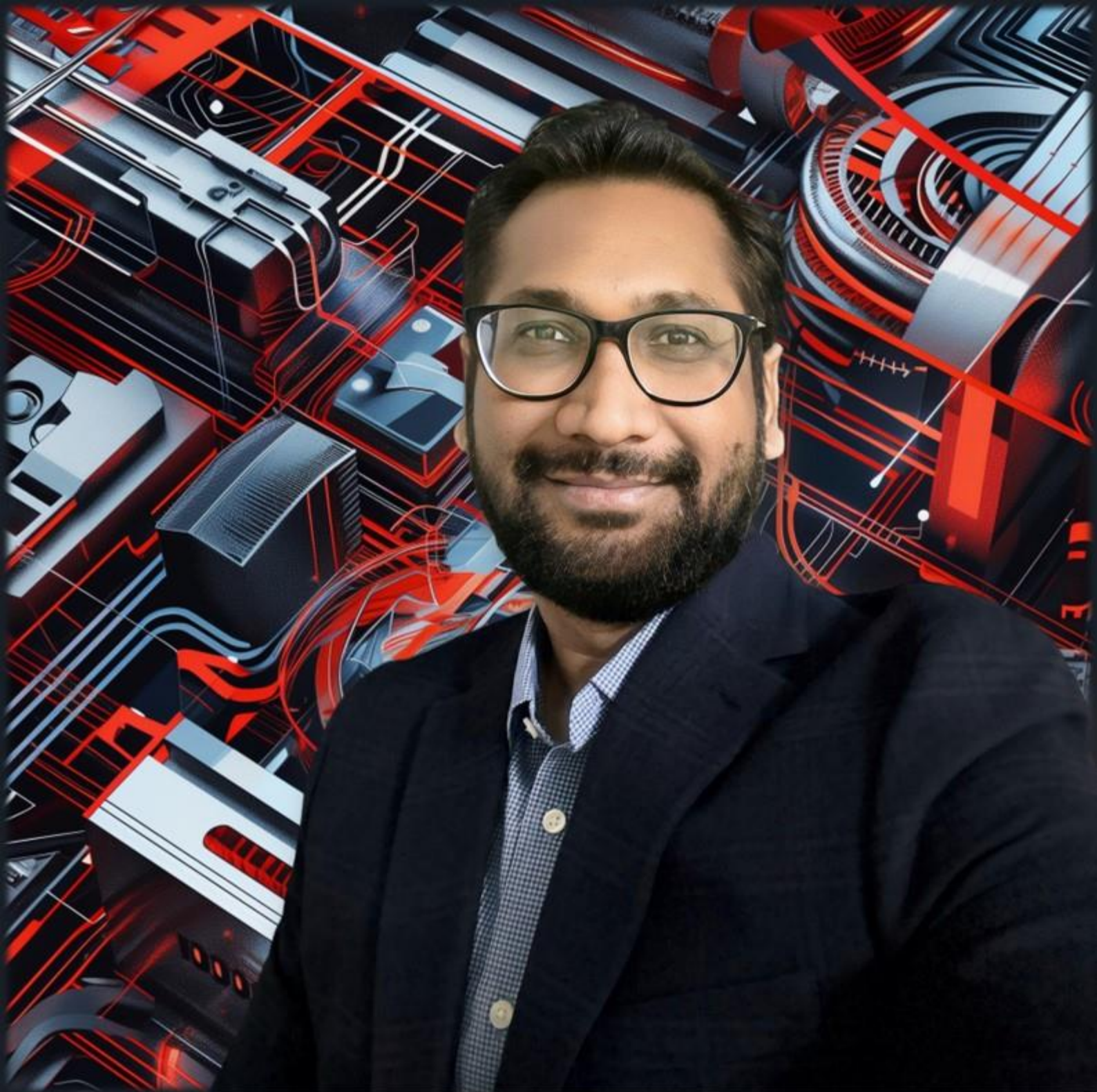
Tackling Explainability Challenges

Deep learning models, while powerful, can be difficult to interpret. This lack of explainability can be a significant hurdle in high-stakes areas like healthcare and finance, where transparency is critical. In these cases, opting for simpler, more interpretable models - such as decision trees - can help meet transparency requirements without sacrificing performance.

Embrace Algorithmic Accountability Now

Algorithmic auditing isn't just about compliance, it's an opportunity to build AI systems that are secure, fair, and transparent. For cybersecurity leaders, this means going beyond data protection to ensure that the algorithms driving key decisions are ethical, explainable, and resilient.

Start by implementing AI governance into your strategy now, and ensure that your AI systems are built to thrive in the era of accountability.



Akhil Mittal, CISSP, CCSP is a recognized cybersecurity leader with over two decades of experience in application security, cloud security, and DevSecOps. As a **Gartner Cybersecurity Ambassador** and **Senior Manager** at **Black Duck**, he leads key security initiatives, helping global organizations strengthen their defenses against advanced cyber threats.

Akhil has worked closely with CISOs and executive leadership to align security strategies with business goals, ensuring robust protection across industries. He also contributes his expertise through leading cybersecurity publications and serves as a judge for top industry awards and hackathons. Certified in **CISSP** and **CCSP**, his work continues to shape the future of cybersecurity, driving innovation and resilience worldwide.

Cybersecurity and Social Responsibility

by **Marta de Zavala**, the UAE and Spain

Christian Felber, promoter of the Economy of the Common Good, once emphasized that *trust is the greatest social and cultural good that we know. Trust is what holds society together in the deepest part, not efficiency.*

In June 2010, the world witnessed a dramatic example of how the intangible world of cyberspace can have a tangible, real-world impact. The Stuxnet computer worm infiltrated the nuclear fuel enrichment plant in Natanz, Iran, causing over 1,000 machines to self-destruct. This cyber-attack served as a chilling reminder of the power of malicious digital threats to wreak havoc on physical infrastructure. Stuxnet, however, was just the tip of the iceberg. In May 2019, Baltimore, a major U.S. city, fell victim to a massive cyber-attack orchestrated by the RobinHood ransomware. This breach left critical systems and infrastructure under the control of hackers for an extended period, disrupting the city's operations and daily life.

When we reflect on these cyber-attacks, it becomes evident that there is a profound human cost associated with them. *Beyond the immediate economic impact, the potential loss of trust, security, and the disruption of societal functions are highly important factors to consider.*

The concept of *Strategic Social Responsibility (SSR)* emerged in 2014, signifying the integration of social responsibility into an organization's strategic orientation and mission, with active involvement from senior management. If we view cybersecurity as a vital component of the positive social impact, a branch essential for the proper functioning of society, it becomes a legitimate candidate for the Strategic Social Responsibility movement.

The trust of clients and citizens in companies and institutions is, as **Christian Felber** already stated, what keeps society together in the deepest part. Perhaps for this reason, *cybersecurity should become the cornerstone of the digital strategy, which puts the human being at the center of the strategy.*

40 under 40 in Cybersecurity by Top Cyber News MAGAZINE, **Marta de Zavala** is a Spanish Cybersecurity expert based in Dubai. She is the **Founder and CEO** of **Cysuite**, a pioneering company dedicated to bridging the gap between cybersecurity and business teams, and of **The Cysuite Method**, a platform aimed at promoting cybersecurity awareness within families.

With a robust educational background in **International Business** and a **Master's degree in Cybersecurity**, Marta's Cyber security career and experience spans across five countries between Europe and the Middle East.

Marta de Zavala has been recognized as a keynote speaker for prestigious international Cyber security institutions, in Europe and the GCC.



Let Us Remember: We Are All Human

AfterWord by **Pooja Shimpi**, India

Wow, 2024 has undoubtedly been the year of Artificial Intelligence. In cybersecurity, we have been flooded with so many ideas about how AI will revolutionize our field. *The narrative was simple: cybercriminals will use advanced AI to conduct more sophisticated attacks, but we can outsmart them by deploying AI to defend ourselves.* However, the reality isn't quite so straightforward and far more complex.

Cybercrimes are getting sophisticatedly crafted by humans, and at the receiving end are also humans. The more I learn about the range of cybercrimes - from petty scams to devastating threats like cyber kidnapping - the clearer it becomes that AI alone will not solve these issues. No matter how advanced technology gets, the human factor will always be at the centre of cybersecurity. As former FBI Director James Comey wisely said, "*The human element is the most unpredictable in cybersecurity - and the most crucial.*" We can utilize AI to enhance our defenses, but unless we educate people about the risks, they unknowingly carry with them, change will be limited.

Security starts with people, not programs and technology, so let us build a safer world together! Addressing human risk in cybersecurity requires a holistic approach, one that should be at the heart of every organization's security strategy. Our goal must be to empower individuals with knowledge as much as we equip them with tools.

Top Cyber News MAGAZINE is doing incredible work by uniting cybersecurity experts across the world and their sharing valuable insights in various areas such as Cybersecurity Awareness, Data Protection, Cyber Hygiene, Ransomware, AI, Deepfake, IoT, Human Risk, Cyber Resiliency, Application Security, Cyber Psychology and more to enlighten the readers.

Thank you, Ludmila, for this wonderful opportunity to be part of this mission.

40 under 40 in Cybersecurity by Top Cyber News MAGAZINE, A globally recognized cybersecurity expert with a strong focus on the human elements of cybersecurity, **Pooja Shimpi** is the Founder and CEO of **SyberNow**. Pooja believes that understanding and strengthening the human aspect of cybersecurity is essential for defending against increasingly sophisticated cyberattacks. Through **SyberNow**, she has pioneered innovative approaches to cybersecurity awareness training, elevating organizational security culture. Their approach involves real-world cybercrimes into engaging narratives, creating a captivating series that educates and entertains. Their innovative method has captured the attention of employees, who eagerly anticipate each new episode, effectively bridging the gap between cybersecurity education and user engagement.

In 2024, Pooja Shimpi was honoured with the **Woman Entrepreneur of the Year Award**, recognizing her exceptional leadership.





TOP CYBER NEWS MAGAZINE

WALL OF FAME

