CyAN
Cybersecurity
Advisors
Network

Cyber (In)Securities

Issue #120

CyAN Cybersecurity Advisors Network

NEWS:

1. US freezes foreign aid, halting cybersecurity defense and policy funds for allies

Original Source: The Register by Jessica Lyon

The U.S. government has frozen foreign aid, including funds allocated to support allies' cybersecurity defense and policy initiatives.

This unexpected move could leave critical infrastructure in allied nations vulnerable, as many rely on U.S. funding for cyber resilience programs and threat intelligence sharing.

The freeze has sparked concern among cybersecurity experts, who warn that delayed assistance could embolden cyber adversaries.

The halt underscores the interconnected nature of global cybersecurity and the need for consistent, collaborative funding.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

2. Apple fixes this year's first actively exploited zero-day bug

Original Source: Bleeping Computer by Sergiu Gatlan

Apple has released emergency updates to patch the first zero-day vulnerability actively exploited in 2025.

The bug, affecting iOS, iPadOS, and macOS, allowed attackers to execute arbitrary code with kernel privileges.

Security experts urge users to update their devices immediately, as the exploit is reportedly being used in targeted attacks.

This incident highlights the persistent risks of unpatched vulnerabilities and the importance of rapid response in securing consumer devices against emerging threats.

CyAN Cybersecurity Advisors Network

NEWS:

3. For $50, Cyberattackers Can Use GhostGPT to Write Malicious Code

Original Source: Dark Reading by Jai Vijayan

A new AI tool called GhostGPT is being sold on underground forums for as little as $50, offering cybercriminals an easy way to generate malicious code.

Unlike ChatGPT, which has safeguards, GhostGPT allows unrestricted outputs, enabling attackers to create phishing emails, malware, and exploit scripts with minimal effort.

The tool is being hailed as a "game-changer" for cybercrime, underscoring the need for stronger controls on AI misuse. Experts call for enhanced monitoring and stricter enforcement to address the growing threat posed by rogue AI tools.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

NEWS:

4. EU sanctions Russian GRU hackers for cyberattacks against Estonia

Original Source: Bleeping Computer by Sergiu Gatlan

The European Union has imposed sanctions on members of Russia’s GRU military intelligence agency for their involvement in cyberattacks targeting Estonia.

These attacks, which disrupted critical services and infrastructure, highlight the ongoing cyber conflict between Russia and EU member states.

The sanctions aim to deter further aggression by freezing assets and imposing travel bans on the individuals responsible.

EU officials stress that these measures reflect the bloc’s commitment to holding nation-state hackers accountable for their actions.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

5. Hackers steal $85 million worth of cryptocurrency from Phemex

Original Source: Bleeping Computer by Bill Toulas

Hackers have stolen $85 million in cryptocurrency from Phemex, a major digital asset exchange, using sophisticated tactics to bypass security measures.

The breach exposed vulnerabilities in Phemex’s systems, and affected users are being urged to monitor their accounts and change credentials.

While Phemex is investigating the incident and collaborating with authorities, the attack highlights the persistent risks facing crypto platforms.

Experts recommend enhanced authentication measures and robust threat detection tools to mitigate future breaches.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

6. Google takes action after coder reports 'most sophisticated attack I've ever seen'

Original Source: The Register by Connor Jones

Google has responded to a highly sophisticated cyberattack reported by a coder, describing it as one of the most advanced they’ve encountered.

The attack involved layered exploits and advanced obfuscation techniques targeting Google’s cloud infrastructure. Google has since patched the vulnerabilities and is investigating the source.

The incident underscores the increasing complexity of modern cyber threats and the critical need for proactive threat detection and mitigation strategies.

CyberSecurity Advisors Network

CyAN
Cybersecurity
Advisors
Network

NEWS:

7. DeepSeek hit with ‘large-scale’ cyber-attack after AI chatbot tops app stores

Original Source: The Guardian by Dara Kerr

DeepSeek, an AI chatbot that recently topped app store charts, has fallen victim to a large-scale cyberattack.

The breach disrupted services and potentially exposed user data, raising questions about the platform’s security measures.

Analysts attribute the attack to the platform’s rapid growth, which may have outpaced its ability to implement adequate protections.

DeepSeek has apologised to users and promised to enhance its security framework.

This incident serves as a cautionary tale for companies scaling rapidly without prioritising cybersecurity.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

NEWS:

8. ‘Sputnik moment’: $1tn wiped off US stocks after Chinese firm unveils AI chatbot

Original Source: The Guardian by Dan Milmo, Amy Hawkins, Robert Booth & Julia Kollewe

The launch of a Chinese AI chatbot has been dubbed a "Sputnik moment," wiping $1 trillion off U.S. tech stocks as investors react to the potential of China surpassing the U.S. in AI innovation.

The chatbot’s unveiling has intensified global competition in AI development, highlighting concerns about technological supremacy and economic impacts.

Analysts warn that this milestone could shift the AI landscape, prompting increased investment and innovation efforts in the U.S. to maintain a competitive edge.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

9. GitHub Desktop Vulnerability Risks Credential Leaks via Malicious Remote URLs

Original Source: The Hacker News by Ravie Lakshmanan

A critical vulnerability in GitHub Desktop has been discovered, allowing attackers to exploit malicious remote URLs to steal user credentials.

The flaw impacts both Windows and macOS versions of the application, posing a significant risk to developers relying on GitHub for code management.

GitHub has released patches to address the issue and urges users to update immediately.

This incident highlights the importance of securing developer tools, as they are increasingly targeted by cybercriminals to gain access to broader systems.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

NEWS:

10. Open-source security spat leads companies to join forces for new tool

Original Source: Cyberscoop by Greg Otto

Amid growing concerns over open-source vulnerabilities, leading companies have collaborated to create a new tool designed to enhance open-source security.

This initiative follows high-profile disputes over accountability in maintaining widely used libraries.

The tool aims to provide real-time monitoring, automated updates, and vulnerability scanning to address gaps in open-source projects.

This collaboration underscores the industry’s recognition of shared responsibility in safeguarding open-source ecosystems critical to global technology infrastructure.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

NEWS:

11. Sweden seizes cargo ship after another undersea cable hit in suspected sabotage

Original Source: The Register by Jude Karabus

Swedish authorities have seized a cargo ship following another incident of undersea cable damage in what is suspected to be sabotage.

The damaged cable disrupted critical communications, adding to concerns over the vulnerability of undersea infrastructure. Investigators are examining whether state-sponsored actors or criminal groups are behind the attacks.

This latest incident highlights the urgent need for enhanced protection of global communication networks and international cooperation to address potential threats.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

12. GamaCopy Mimics Gamaredon Tactics in Cyber Espionage Targeting Russian Entities

Original Source: The Hacker News by Ravie Lakshmanan

A new cyber espionage campaign dubbed "GamaCopy" is mimicking the tactics of the Gamaredon group to target Russian entities.

The campaign uses phishing emails and malware-laced documents to steal sensitive information. Security experts believe the threat actors aim to obscure their identities by replicating known techniques.

Organisations are advised to implement advanced threat detection systems and educate employees on phishing risks.

This incident highlights the evolving strategies of cybercriminals to remain undetected while targeting high-value entities.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

NEWS:

13. Change Healthcare Data Breach Exposed the Private Data of over Half the U.S.

Original Source: Security Affairs by Pierluigi Paganini

A data breach at Change Healthcare has exposed sensitive personal and medical information for over half the U.S. population.

The breach impacted data stored in its systems, including health records, billing details, and insurance information. Security experts warn that this incident poses a significant risk of identity theft and fraud.

Change Healthcare is working to mitigate the fallout and improve its security posture.

The breach underscores the vulnerabilities in healthcare systems and the critical need for stronger data protection measures.

Cybersecurity Advisors Network

NEWS:

14. SonicWall warns hackers targeting critical vulnerability in SMA 1000 series appliances

Original Source: Cybersecurity Dive by David Jones

SonicWall has issued an urgent warning about a critical vulnerability in its SMA 1000 series appliances, which attackers are actively exploiting.

The flaw allows remote code execution, enabling cybercriminals to gain control of affected systems. SonicWall has released patches and advises users to update immediately.

This incident highlights the risks of delaying critical updates and the importance of regular vulnerability scanning in enterprise environments.

Organisations are urged to prioritise patch management to prevent potential exploitation.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

15. UnitedHealth hikes number of Change cyberattack breach victims to 190M

Original Source: Cybersecurity Dive by Emily Olsen

UnitedHealth has disclosed that 190 million individuals were affected by the cyberattack on Change Healthcare, significantly increasing the initially reported figure.

The breach involved sensitive data, including patient records and financial information.

This update raises concerns about the scale of the attack and its long-term impact on victims.

UnitedHealth is working with regulators to address the fallout, but the incident serves as a wake-up call for better security investments in the healthcare sector.

CyberSecurity Advisors Network

ANALYSIS:

16. Cyber Insights 2025: Cybersecurity Regulatory Mayhem

Original Source: Security Week by Kevin Townsend

This analysis explores the growing complexity of global cybersecurity regulations heading into 2025.

Organisations are struggling to navigate overlapping frameworks, from GDPR to the latest mandates on AI and data governance.

The article highlights the importance of proactive compliance strategies, as falling behind could mean severe penalties and reputational damage.

With governments introducing more sector-specific rules, businesses need to embrace agility and cross-border collaboration to stay compliant and competitive.

ANALYSIS:

17. Post-Quantum Cryptography 2025: The Enterprise Readiness Gap

Original Source: ISMG Data Breach Today by Sandhya Michu

As post-quantum cryptography gains traction, enterprises are facing challenges in readiness and implementation.

This analysis highlights a significant gap in preparation, with many organisations struggling to transition to quantum-safe encryption standards.

The article urges leaders to prioritise migration strategies, invest in workforce education, and collaborate with industry groups to accelerate readiness.

Early adoption of post-quantum solutions will be key to safeguarding sensitive data against future quantum computing threats.

CyberSecurity Advisors Network

Cybersecurity Advisors Network CyAN

ANALYSIS:

18. World Economic Forum 2025: Navigating Cybersecurity in an Era of Complexity

Original Source: Lohrmann on Cybersecurity by Dan Lohrmann

At the 2025 World Economic Forum, cybersecurity took centre stage as leaders grappled with the complexities of an interconnected digital economy.

Discussions focused on global collaboration, AI-driven cyber threats, and strengthening critical infrastructure resilience.

The article emphasises the need for public-private partnerships to address emerging risks and foster trust across industries.

With cyberattacks becoming more sophisticated, the forum highlighted the urgency of proactive strategies to ensure a secure digital future.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

ANALYSIS:

19. Navigating The Next Frontier Of Email Threats: Five Emerging Attacks Shaping Cybersecurity In 2025

Original Source: Forbes by Mike Britton

This analysis highlights five emerging email-based cyber threats poised to dominate 2025, including AI-driven phishing, business email compromise (BEC) 3.0, and deepfake-enabled scams.

As attackers evolve their tactics, businesses face greater challenges in protecting communication channels. The article stresses the importance of advanced threat detection tools and employee training to counter these risks.

Organisations that prioritise innovation in email security stand a better chance of staying ahead of these sophisticated attacks.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN CyAN Members Op Eds, Articles, etc

20. China's Open-Source AI: The genie is out of the bottle, and the race is on

Original Source: Kim Chandler McDonald

CyAN global VP Kim Chandler McDonald explores the transformative impact of China’s open-source AI revolution on global geopolitics, economics, and investment strategies.

By leveraging open-source innovation, China is rapidly altering the balance of technological power, sparking heightened competition in AI development.

The article examines how these advancements are not only disrupting global markets but also influencing international investment flows and prompting shifts in AI funding priorities.

Kim calls for stakeholders worldwide to reassess their strategies in light of China’s ambitious push, framing the race as a pivotal moment for global economic and technological leadership.

Cybersecurity Advisors Network

CyAN CyAN Members Op Eds, Articles, etc

21. Criminal hackers, QILIN Ransomware Group

Original Source: Dan Elliot

CyAN member Dan Elliot provides an in-depth look at the QILIN ransomware group, notorious for its sophisticated double-extortion tactics.

The group targets enterprises by encrypting data and threatening to leak sensitive information if ransoms aren't paid.

Dan highlights their evolving techniques, including leveraging advanced encryption and social engineering to increase their success rate.

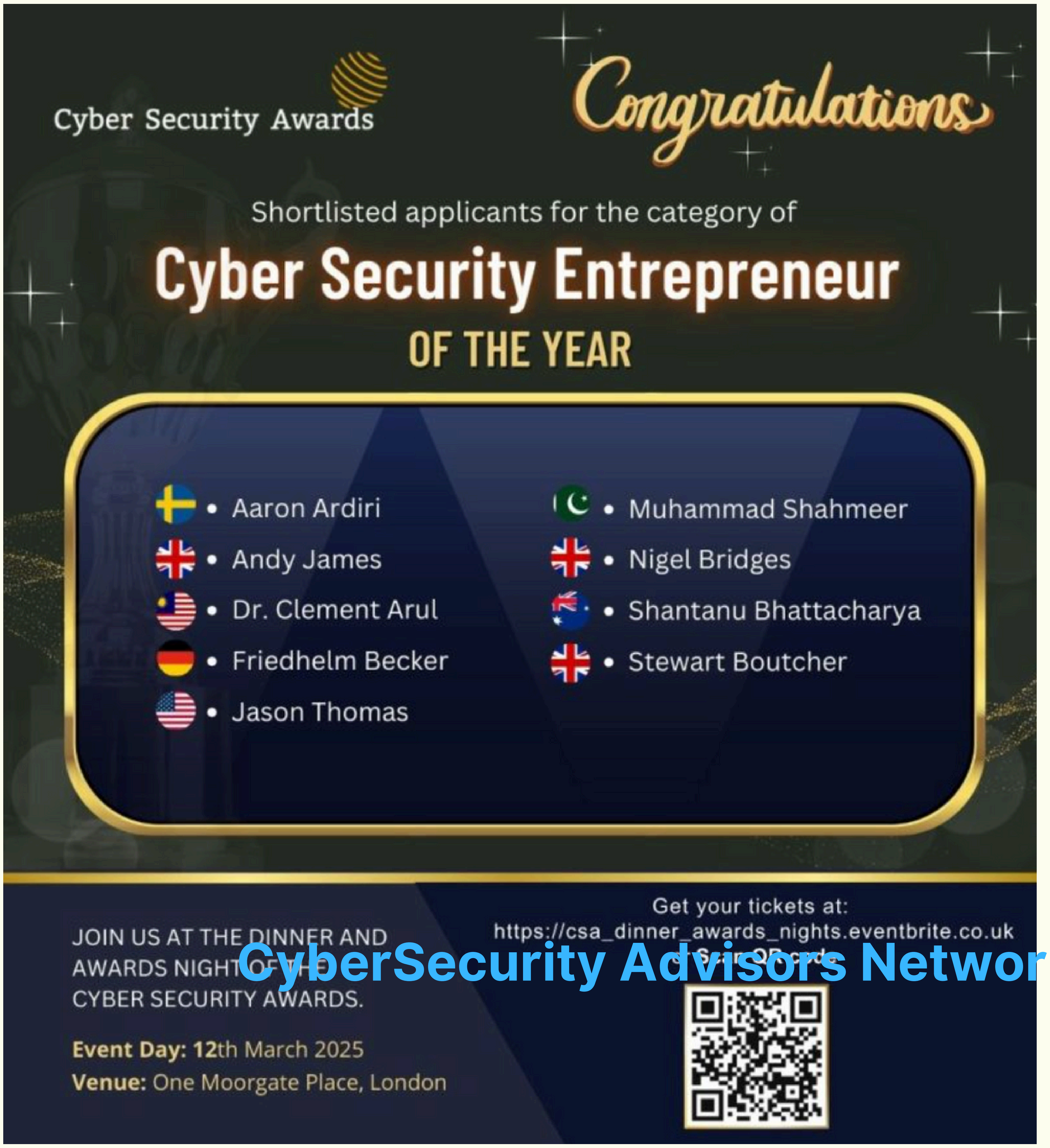
The article serves as a critical reminder of the need for strong incident response plans and robust cybersecurity measures.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN NEWS:

Congratulations to CyAN member Shantanu Bhattacharya on his nomination for Cyber Security Entrepreneur of the Year at the Cyber Security Awards!



Cyber Security Awards

Congratulations

Shortlisted applicants for the category of

Cyber Security Entrepreneur OF THE YEAR

- Aaron Ardiri
- Andy James
- Dr. Clement Arul
- Friedhelm Becker
- Jason Thomas
- Muhammad Shahmeer
- Nigel Bridges
- Shantanu Bhattacharya
- Stewart Boutcher

JOIN US AT THE DINNER AND AWARDS NIGHT OF THE CYBER SECURITY AWARDS.

Event Day: 12th March 2025

Venue: One Moorgate Place, London

Get your tickets at:
https://csa_dinner_awards_nights.eventbrite.co.uk
or Scan QR code

CyAN Cybersecurity Advisors Network

CyAN Mentorship Program 2025:

At CyAN, we believe mentorship is a powerful tool to nurture future leaders and strengthen our global community.

Our structured three-month mentorship program offers professional guidance, international networking opportunities, and real-world insights tailored to support graduate students and early-career professionals.

By connecting with experienced CyAN members, mentees gain invaluable skills and perspectives to advance their careers.

If you’re ready to grow, learn, and thrive alongside experts in cybersecurity and trust & safety, we encourage you to join this transformative opportunity.

UPCOMING EVENTS:

- AI Global Everything, Dubai, UAE: 4-6 February
- CyAN APAC: The Geopolitical Impacts of Cyber Threats: From Espionage to Influence keynote by Dan Elliot, March 12, Peoplebank, Sydney (save the date, tickets available soon!)
- GITEX AFRICA, Marrakesh, Morocco: 14-16 April
- GITEX ASIA: Singapore (Marina Bay Sands) 23-25 April
- GISEC: Dubai Word Trade Center, Dubai, UAE: 6th to 8th May
- The Cyber Outstanding Security Performance Awards (Cyber OSPAs), May 8, London, UK
- MaTeCC, Rabat, Morocco: 7-9 June, 2025 hosted by CyAN partner organisation École High-Tech.

CyAN Cybersecurity Advisors Network

Catch up on Past Issues:

Missed an issue of (In)Securities? No worries! Scan the QR code to explore our archive of past editions—packed with insights, trends, and actionable tips to keep you ahead in the ever-evolving world of cybersecurity. Dive in and catch up today!

CyberSecurity Advisors Network

If you found this interesting, please like and share it with your friends and colleagues!

#ReallyInterestingCyberStuff!

#SharingIsCaring