



**SECURITY
DAYS**

DON'T WORRY, IT'S ONLY GETTING WORSE

AI, SOCs & OPTIMISM IN AN UNCERTAIN WORLD

Dave Maasland,
ESET Nederland CEO

"The most important **failure** was one of **imagination**. We do not believe leaders understood the gravity of the threat."

- FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES



Handwritten text in a cursive script, likely a description of the device above. The text is written in a language that appears to be a form of Arabic or Persian, with some characters resembling 'S' and 'A'. The script is somewhat faded and difficult to decipher precisely.

Handwritten text in a cursive script, likely a description of the device below. The text is written in a language that appears to be a form of Arabic or Persian, with some characters resembling 'S' and 'A'. The script is somewhat faded and difficult to decipher precisely.

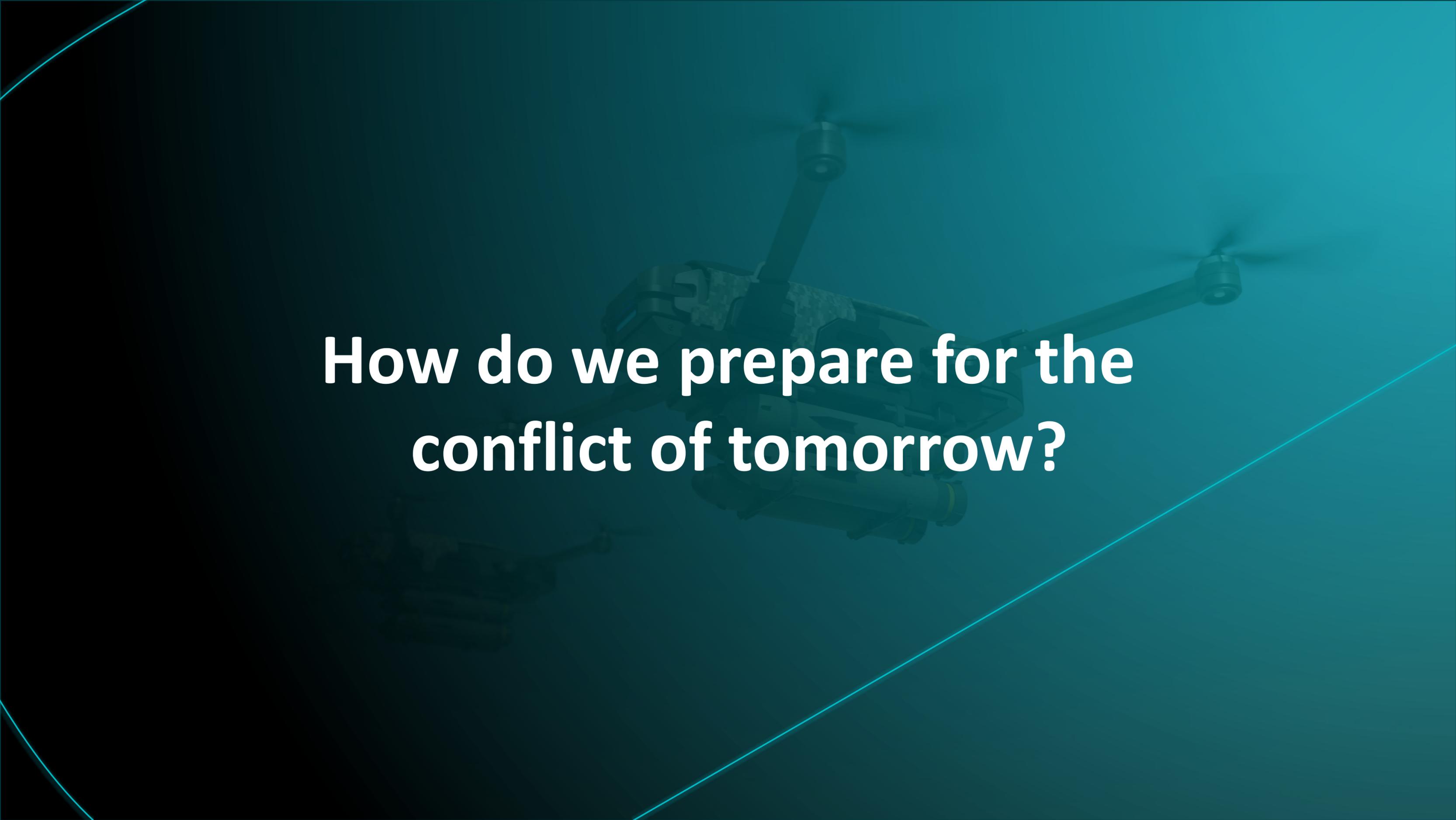




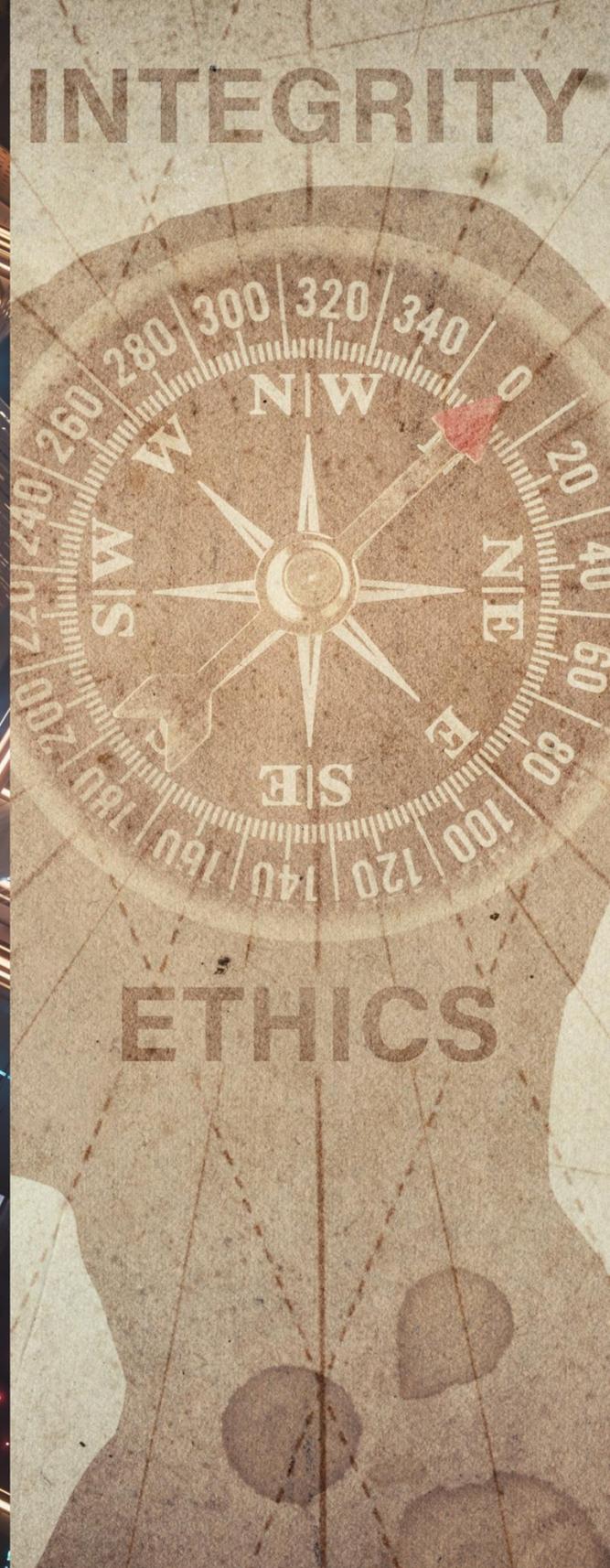
Cybercrime is not a cat & mouse game



Technology gives superpowers to both sides

A blurred image of a drone in flight against a teal background. The drone is positioned in the center-right of the frame, with its four propellers visible. The background is a solid teal color with a subtle gradient and some faint, abstract lines.

**How do we prepare for the
conflict of tomorrow?**



What we don't know...



What we do know...

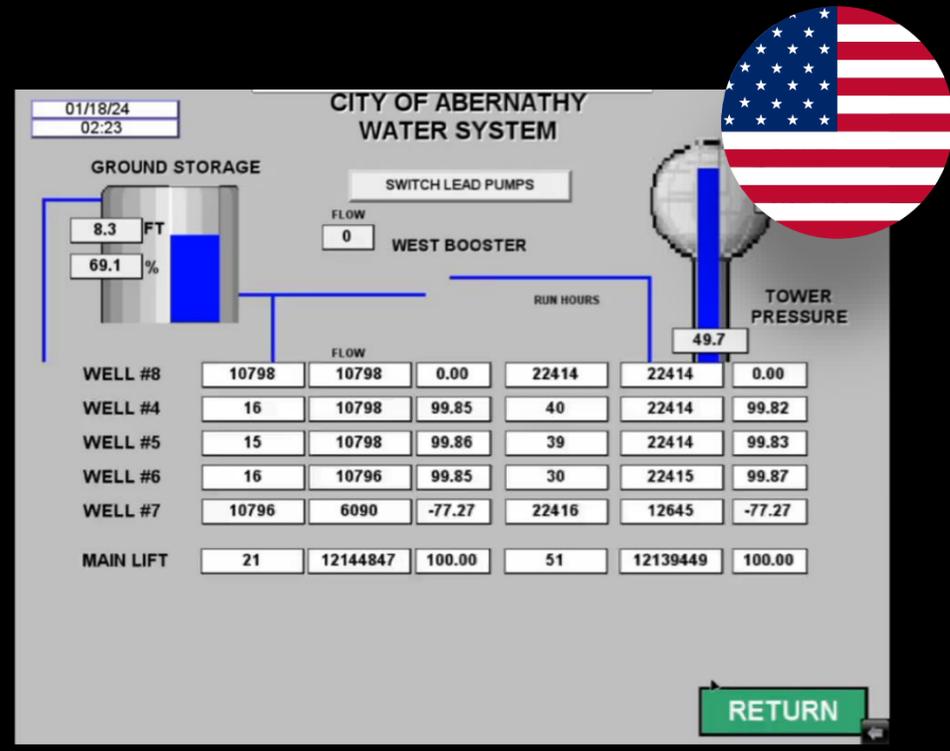
AI & Technology isn't just transforming what we use - it's reshaping who holds power, how wars are fought, what we believe, and who we trust.

The logo for LockBit 3.0 ransomware. It features a stylized white 'B' with a black outline and a red shadow, set against a dark blue background with red, organic, vein-like patterns. Below the 'B' is the text 'LOCKBIT 3.0' in white, with 'BIT' highlighted in a red rectangular box.

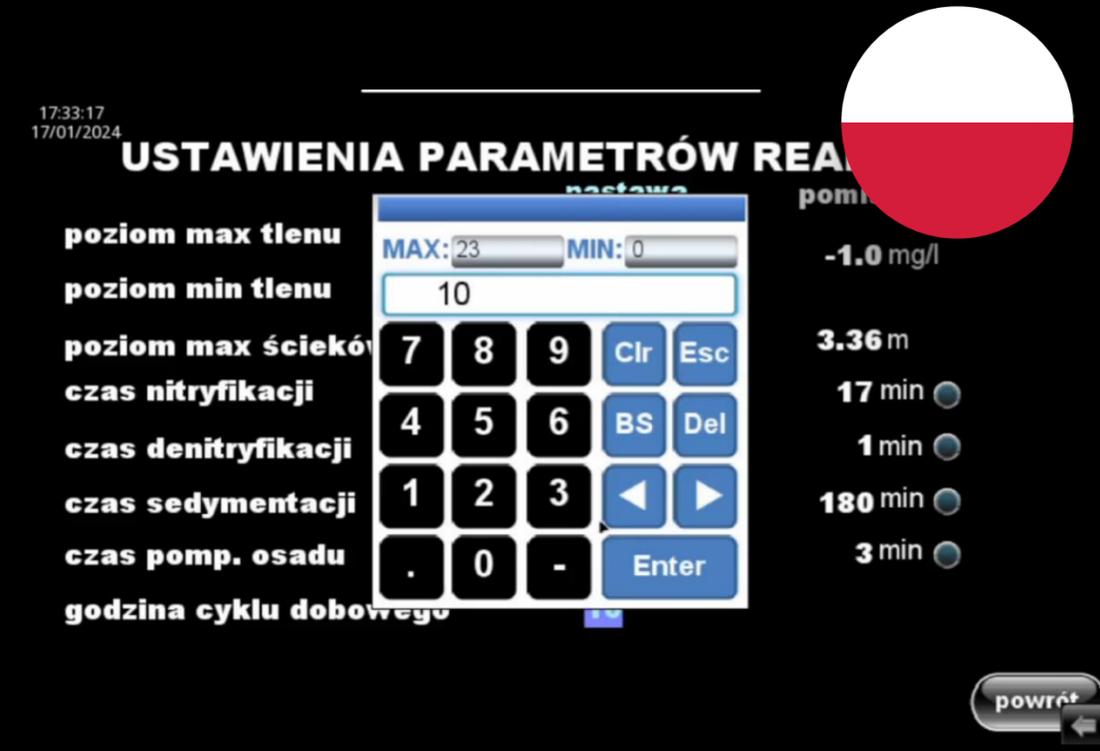
LOCKBIT 3.0



Power doesn't just belong to big states, corporations, or institutions anymore — AI and technology are flipping that idea.



Multiple US water utilities in Texas

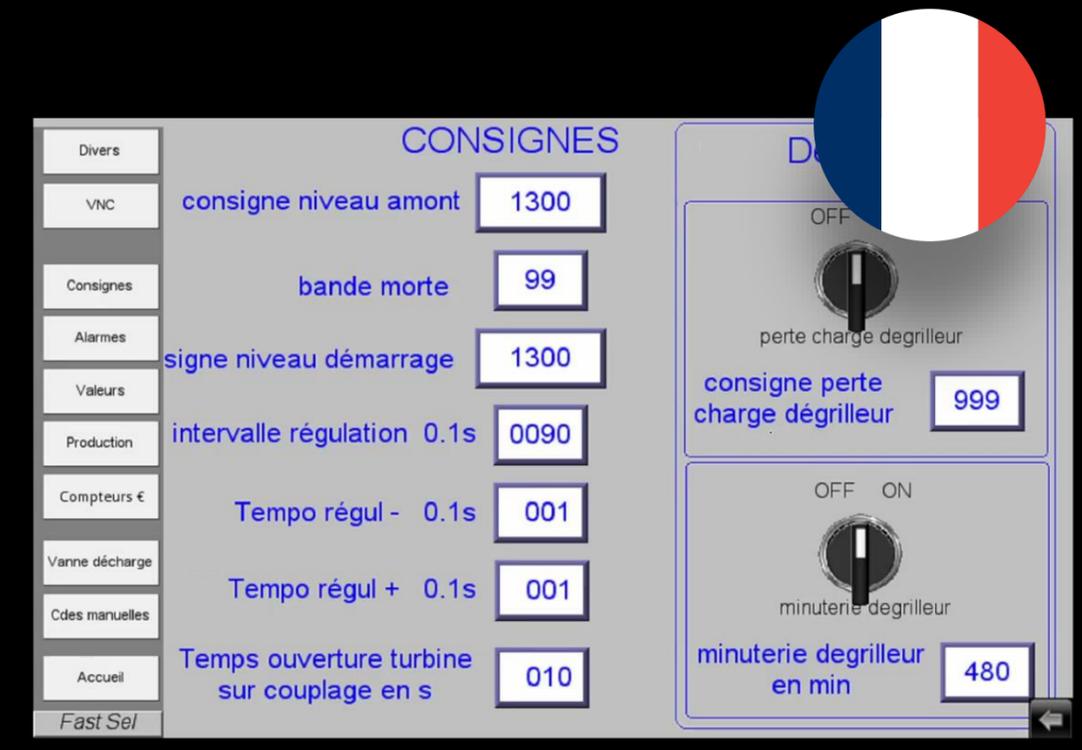


Polish wastewater treatment plant



CyberArmyofRussia_Reborn

Source: Wired



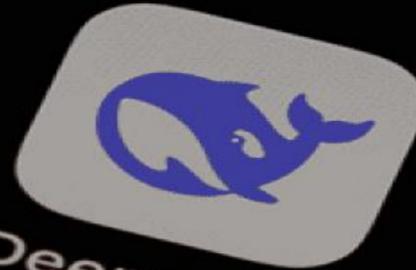
French hydroelectric plant

Hacktivism isn't about technical disruption. It's about emotional disruption

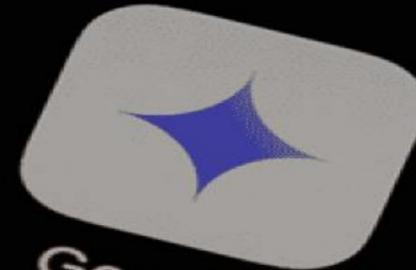
17:49



ChatGPT



DeepSeek



Gemini



64

WAR IN UKRAINE

Researchers Reveal How Russia's Propaganda Network "Infects" Leading AI Chatbots

"They Got Watches, We Got Time"



Our Democracy Itself Is The Main Target

No one is immune to disinformation If everything is right...



Emotional involvement

An influencer

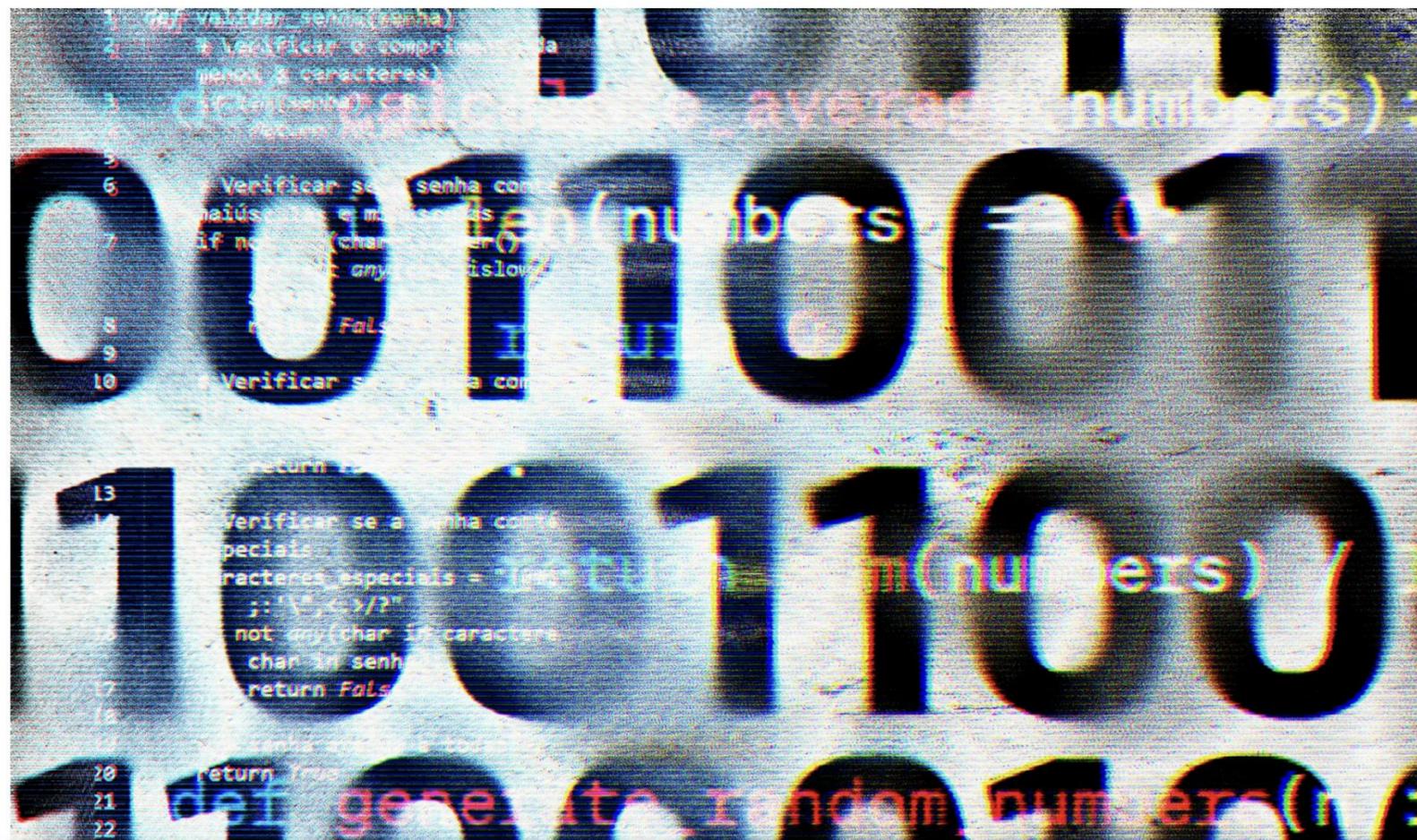
"Proof"

How Threat Actors Are Leveraging – HIGH LEVEL

LILY HAY NEWMAN MATT BURGESS SECURITY AUG 27, 2025 8:36 AM

The Era of AI-Generated Ransomware Has Arrived

Cybercriminals are increasingly using generative AI tools to fuel their attacks, with new research finding instances of AI being used to develop ransomware.



How Threat Actors Are Leveraging – HIGH LEVEL

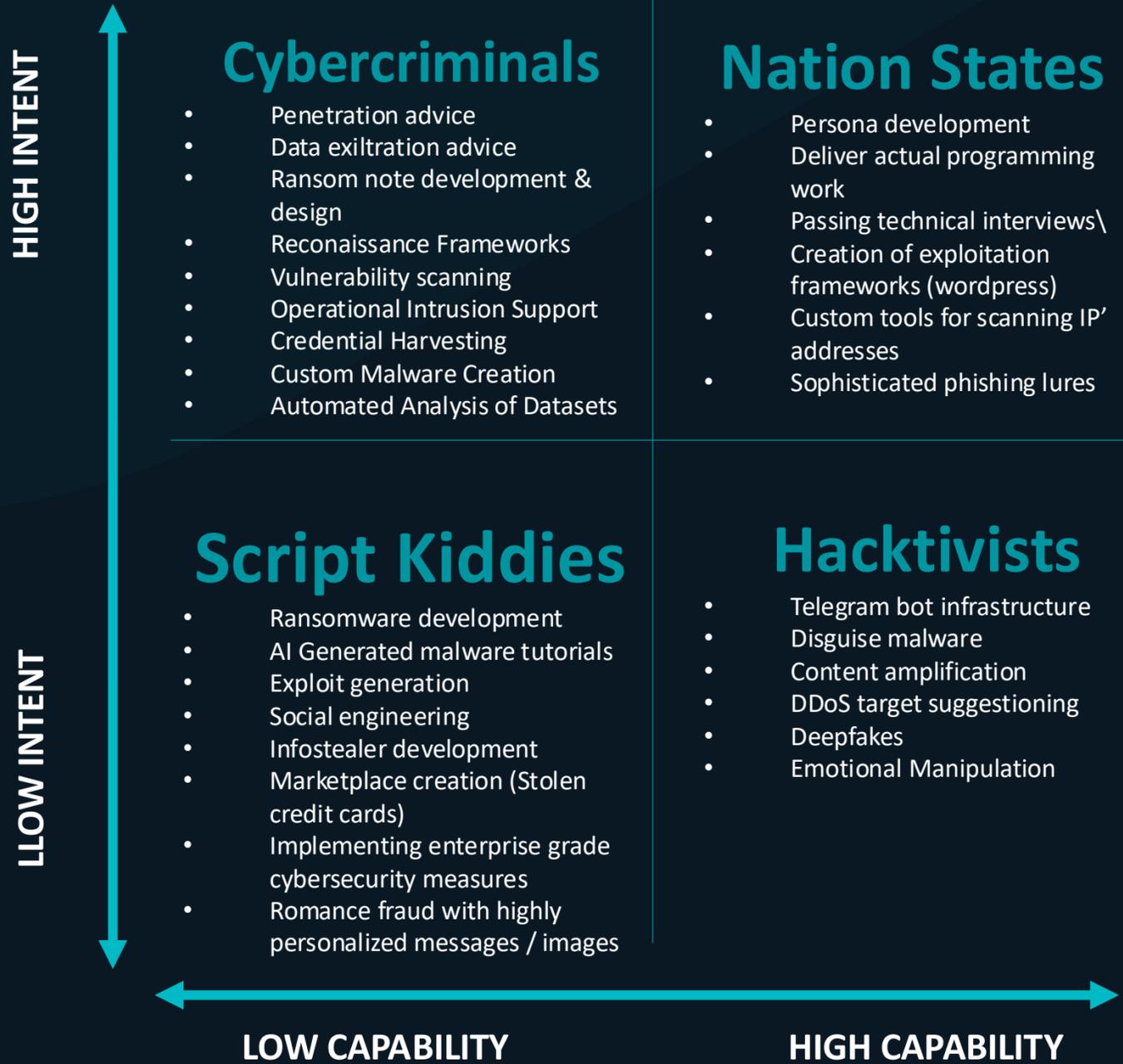
- **Agentic AI systems are being weaponized:**
AI models are themselves being used to perform sophisticated cyberattacks – not just advising on how to carry them out.
- **AI lowers the barriers to sophisticated cybercrime.**
Actors with few technical skills have used AI to conduct complex operations, like developing ransomware, that would previously have required years of training.
- **Cybercriminals are embedding AI throughout their operations.**
This includes victim profiling, automated service delivery, and in operations that affect tens of thousands of users.
- **AI is being used for all stages of fraud operations.**
Fraudulent actors use AI for tasks like analyzing stolen data, stealing credit card information, and creating false identities.

AI has become the co-pilot of cybercrime —
in every stage, for every actor.

ANTHROPIC

Threat Intelligence Report: August 2025

How Threat Actors Leverage AI – Detailed View



✔ AI executes complex attacks autonomously

✔ One actor equals an entire cybercrime team

✔ AI selects targets, tactics & monetization

✔ AI adapts in real-time to your defenses



The real question isn't how to calm the storm, but how to build a house of stone that stands through it



A SOC is not a tool — it's a function designed to raise your security posture to a level where your business can withstand the storm



BUSINESS

RISK

TECHNOLOGY



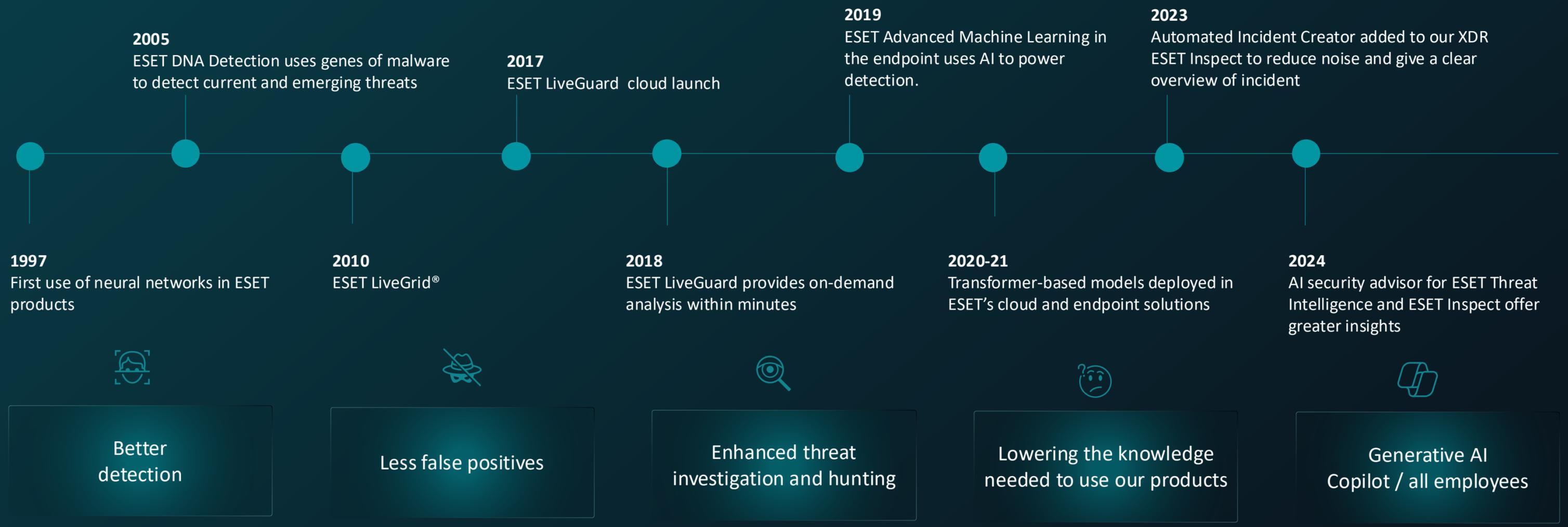
SOC of the PAST

- Focused on tools, systems, and technology
- Reported on technical problems
- Measured success by alert volume
- Treated AI as a silver bullet
- Worked in silos (IT only)

SOC of the FUTURE

- ✓ Aligned with business strategy and risk
- ✓ Links incidents to strategic business outcomes
- ✓ Measures impact by risk reduction
- ✓ Uses AI to accelerate decision-making and free up human expertise
- ✓ Embedded across the organization

AI in ESET Products & Services



Stats & figures

65 TB
of precisely classified binaries

17 MB
of highly optimized AI module distributed to customers

every 8 days
of input preparation, deeplearning and testing

750 000
suspicious samples received every day

60 000 000
metadata records processed every day

2 500 000 000
URLs analyzed every day

Tell me about Russian APT attacks outside of Ukraine

You



ESET AI Advisor

Russian APT groups have been active outside of Ukraine, targeting various sectors and regions across the globe. Here are some key points from the ESET Threat Intelligence reports:

- 1. Sednit (also known as APT28 or Fancy Bear):** Linked to the GRU, Sednit has been active since at least 2004 and is known for high-profile incidents such as the DNC hack. Sednit has been observed launching spearphishing campaigns against governmental entities in EU countries and a defense firm in Poland
- 2. The Dukes (also known as APT29 or Cozy Bear):** This group has been active for more than a decade and is known for its cyberespionage activities. The Dukes have been linked to new Cobalt Strike C&C servers and have targeted European diplomats and ministries.

3. Sandworm Group: Active since at least 2013, Sandworm has been primarily targeting critical governmental institutions but has also been observed launching spearphishing campaigns and conducting its malware tools to target various entities of interest. Sandworm has been attributed by the Cybersecurity Service Center to the 2018 election of information security of the FBI, operating out of unregistered servers.

- 4. Sandworm:** Known for its destructive attacks, Sandworm has been linked to

AI-powered threat detection and analysis

eset PROTECT & INSPECT

QUESTIONS DISABLED HELP LOG OUT

BACK Suspected Malware Execution and Botnet Activity on ei-mgr-test-endpoint-1

Incident graph Timeline Detections Computers Executables Processes Incident Timeline Assistant

What data or information was accessed or exfiltrated?

The data accessed or exfiltrated includes a dropped executable named make-nearmiss.exe, which was flagged as similar to known malware but not confirmed as malware yet. Additionally, suspected botnet activity with the threat name Win32/BotnetProtectionTest was detected from source IP 127.0.0.1 to destination IP 127.0.0.1, initiated by the user ei-mgr-test-endpoint-1 -mgr-t\administrator through httpclienttester.exe, which was blocked due to its unknown reputation and lack of signature.

IMPORTANT: Generated by AI. Verify information for accuracy.

What is the reputation of the dropped executable make-nearmiss.exe?

The dropped executable make-nearmiss.exe has a reputation of "trusted."

IMPORTANT: Generated by AI. Verify information for accuracy.

any more suggestions?

1. Can you provide more details about the source IP 127.0.0.1 and the destination IP 127.0.0.1 in the suspected botnet activity?
2. What action was taken in response to the suspected botnet activity with the threat name Win32/BotnetProtectionTest?
3. Can you provide information about the process httpclienttester.exe and its reputation?

IMPORTANT: Generated by AI. Verify information for accuracy.

Ask ESET AI Advisor anything...

Responses are generated by AI. Verify information for accuracy.

INCIDENT REMEDIATION COMMENT EDIT ASSIGN PROGRESS GRAPH

COLLAPSE

**The old SOC told us what went
wrong.**

**The new SOC helps us decide what
to fix and why.**

AI in the modern SOC?

Accelerate

AI accelerates decision-making — not replaces it

Noise Reduction

Prioritized Alerts

Context-Rich

Real-Time Correlation

Understand

AI turns data into understanding

Telemetry to insight

Risk Mapping

Behavioral Intelligence

Business Context First

Empower

AI frees up human capacity

Automated Triage

Pre-Enriched Alerts

Playbook Execution

Human-in-the-Loop Focus

BONUS INSIGHT: The real problem isn't detection. It's response

"Yes - things may get worse. But how we respond is what defines us. And I believe we are more prepared than we think - if we choose to act now."

- WHY I'M STILL POSITIVE AND YOU SHOULD NOT WORRY

FOR ALL SECURITY PROFESSIONALS

- ✔ **Keep it simple.**
If you can explain it simply, you can make real impact.
- ✔ **Technology is not the goal.**
You're doing this for people, for organizations, for society.
- ✔ **Learn to speak the language of business.**
That's what makes you valuable — a true bridge builder.
- ✔ **Embrace the underdog mindset.**
Even with limited resources, you can create massive impact.
- ✔ **Cyber is a lighthouse for the future.**
You're not just defending — you're guiding others forward.

Prevention still works

- ✔ Patch fast
- ✔ MFA everywhere, no excuses
- ✔ Harden what you own





If you can't win, make sure you can't lose.

How every business can be part of the SOC of our society?

Share

Share what you see — become an early warning system

Don't keep incidents to yourself. When you share IOCs, patterns, and anomalies, you help protect the ecosystem, not just your own network.

Speak Up

Speak up when something feels wrong — report, don't wait

Whether it's phishing, fraud, disinformation or digital abuse — resilience starts with eyes open and voices raised.

Invest

Invest in readiness — not just for you, but for others

Build your internal capacity, but also support local initiatives, startups, and joint efforts that strengthen societal cyber resilience.



Why I'm Still Positive and We Should Not Worry



In Summary

- ✔ **Imagine the conflict of tomorrow** — because what you can't imagine, you can't defend against.
- ✔ **Invest in scenarios rooted in business context** — because resilience isn't about reacting to threats, but about understanding which ones can truly disrupt your mission.
- ✔ **Focus on what *you* can control — and do it well.** Prevention is still the most powerful move you can make.

You Can't Defend What You Refuse To
Imagine



“Imagining is a
boardroom
responsibility.”

The World Is A Fine Place and Worth Fighting For