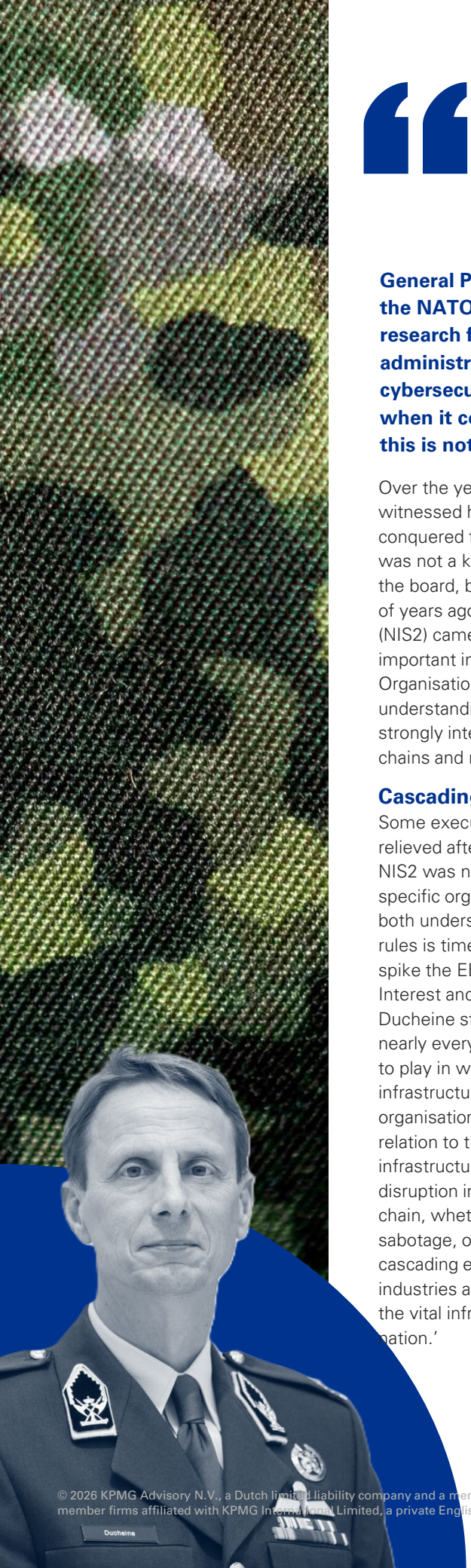
KPMG

Europe at a crossroads

If you think cyber warfare is not about you, think again

General Paul Ducheine

February 2026



If you think cyber warfare is not about you, think again" General Paul Ducheine

General Paul Ducheine is (among other roles) senior researcher at the NATO Defence College in Rome and has been conducting research for more than 10 years on military, operational, administrative, and legal aspects of digital operations and cybersecurity. He urges executives to look beyond their daily grind when it comes to warfare via digital infrastructures. "If you think this is not about you, think again."

Over the years, Ducheine has witnessed how cyber resilience conquered the boardroom. Initially, it was not a key issue on the agenda of the board, but this changed a couple of years ago. European legislation (NIS2) came into effect and was an important impulse for this. Organisations needed better understanding of how they are strongly interconnected in supply chains and networks.

Cascading effects

Some executives were clearly relieved after analysis learned that NIS2 was not applicable to their specific organisation. This relief is both understandable, playing by the rules is time consuming and does not spike the EBIT (Earnings Before Interest and Taxes), as it is worrying. Ducheine stresses the fact that nearly every organisation has its role to play in warranting a resilient critical infrastructure. "Even if you think your organisation is not important in relation to the resilience of vital infrastructures: think again. A disruption in one part of the supply chain, whether due to a cyberattack, sabotage, or even a strike, can have cascading effects across entire industries and thus have impact on the vital infrastructure of a whole nation.'

It is however a common mistake at many companies to underestimate their strategic importance in this respect. A bakery, laboratory or local construction company may not be a valuable target in cyber warfare themselves but could play a role in supply chains that makes them attractive to being used as pawns in broader conflicts. And precisely because these companies lack the awareness about their role, attackers may perceive them as an easy starting point, or entry point, for disturbing vital sectors.

Ducheine knows that in itself, all of this is nothing new. But the message needs to be reinforced time and time again. Of all people, he knows how important it is.

When Ducheine did extensive research about four years ago, he was somewhat surprised by the extent to which IT companies had become central players in armed conflicts between states. **"IT services are the lifeblood of both businesses and governments but are precisely for that reason also an Achilles heel.** Cloud providers and software vendors are now as strategically important as traditional infrastructure such as energy networks. And the rapid advent of AI accelerates the hyperconnectedness. In other words: everyone should play their part to protect the whole. More than ever before in history."

Beyond opportunism

Do you as a board member truly understand how your organisation is positioned? Ducheine is convinced that leaders are focused on short-term growth rather than long-term ambitions, including warranting resilience. "They have a multitude of important topics on their plate and tend to delegate the cyber topics to specialists. By doing so, they completely ignore the strategic importance of it. The communications backbone of any organisation can be the, intermediate, target to ruin the service or product, And the workforce may be lured or blackmailed into malicious acts. Hence, the company's very survival is at stake."

"It's time to wake up and invest proactively", says Ducheine. "In the past few years, we have seen how incidents acted as an effective catalyst for change in individual cases. However, this should not be the primary reason to raise the bar. Instead, **leaders must proactively foster a culture of preparedness, continuous learning, and cross-sector collaboration."**

Cyber in the military doctrine

Nonetheless, Ducheine is also positive about how cyber warfare has evolved from a niche concern to a core pillar of national security in the past decade. "The early days were marked by the challenge of building structures, creating awareness, and overcoming scepticism within traditional defence circles. A key milestone was the formation of the Defence Cyber Command and the integration of cyber strategy into broader military doctrine. Our journey was not without friction: different stakeholders had competing interests." He uses the metaphor of a sports hall with different coloured lines for each sport to illustrate the complexity of cyber: each team plays its own game, with its own rules and objectives, yet they share the same space and sometimes the same players. **Mastering cyber operations requires not just technical skills, but also the ability to collaborate across disciplines** and organisations. And to understand the rules of the different games.

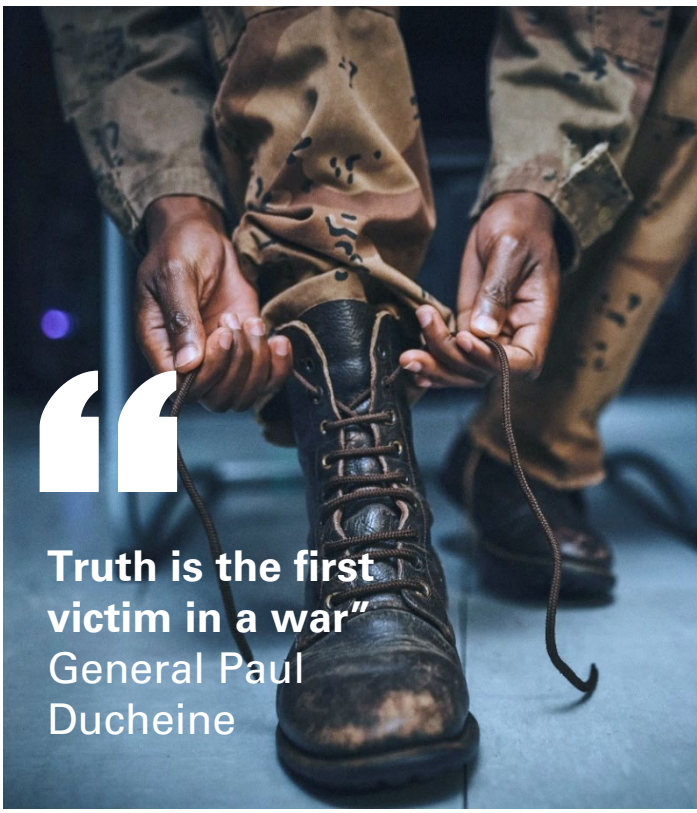
If we use that metaphor in the cyber arena, could we say that the best players are decathletes, not specialists? "Effective cyber defence and offence is a team sport. Ultimately, the goal is to create a team that can respond effectively to both routine and crisis situations, leveraging diverse skills and perspectives. We must encourage rotation and cross-training to improve collaboration across disciplines. The game is not just about technical mastery but also about mutual respect, understanding language, and the ability to operate seamlessly across organisational boundaries."

The power of perception: how disinformation eats trust

Ducheine also reflects on a somewhat overlooked aspect of cyber warfare: the softer approach by influencing public opinions. He points out that Russia and China have been masters of strategic deception throughout history and that technology offers them a vast potential to further ignite polarisation within European societies, which is one of the main goals of Putin. "The value of objective information is actively being eroded by a flood of opinions, impressions, and deliberate misinformation and nation states continuously play a role in this. **The cocktail of AI tooling and social media offers them vast potential to shape, amplify or distort narratives."**

Understanding facts requires more effort than consuming simple one-liners and short (fake) videos and most people don't take the time to dig deeper. This contributes to polarisation in societies. Public perception can diverge from official statistics, which underscores how influential information operations can be.

A well-known historic quote about war is that **'truth is the first victim in a war',** so the efforts to manipulate public perception have been around for ages. But yet again, technology offers a new toolkit to effectively use this weapon. "Gathering intelligence by nation states was once purely done for internal purposes, now it is also useful for obtaining exposure and a suitable narrative. Perhaps the most dangerous poison is invisible disinformation that slowly eats trust."



ESET threat intelligence

Cyber threats are increasingly geopolitical, with state actors such as Russia, China, Iran, and North Korea using cyber operations as a strategic tool worldwide.

Russia-aligned APTs (Advanced Persistent Threat) are seen targeting NATO critical infrastructure and Ukraine supporting countries, including ports, energy and telecommunications, with the objective of destabilisation and disruption of military aid provision.

The Netherlands remains a critical transit hub and is of paramount strategic importance for the sustained support of Ukraine. That comes with an elevated threat profile.

In a landscape of interconnected ecosystems, any organisation within a strategic supply chain is viewed as a legitimate target. And cyber operations have become an integral instrument of geopolitical pressure, including influence operations and disinformation.

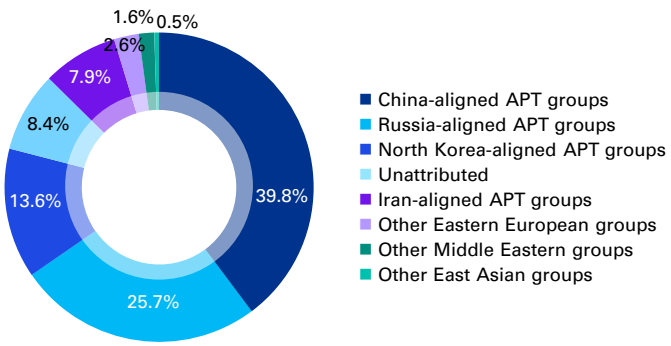
Stats

Ransomware deployment speed accelerated 48 percent (average 24-hour intrusion), driven by commoditisation of initial access and credential theft at scale.

ESET Research projects a 40 percent year-on-year increase in the number of ransomware victims compared to the previous year.

Targeted sectors in Europe

Attack sources



Source: ESET Threat Report H2 2025

Recommendations

Immediate

The board must reframe cybersecurity as a strategic part of the board agenda by establishing a dedicated committee that reports monthly. This ensures that strategic decisions are no longer delegated solely to technical specialists.

Mid-term

Organisations should undertake comprehensive, NATO-aligned cyber resilience audits to identify and eliminate single points of failure within their supply chains and logistics networks. The aim is to prevent cascading effects on critical infrastructure and security of a society in general.

Long-term

As a long-term strategic imperative, organisations must prioritise transforming their IT landscape from a fragile house of cards into a robust, compartmentalised system. This requires a migration of critical systems towards resilient, disaggregated architectures that are resistant to widespread compromise.