Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

War of the machines – how artificial intelligence has taken over cyber operations

Until just a few years ago, serious cyber-attacks still depended on humans. Behind major operations were teams of intelligence officers, state-supported hackers, criminal groups or private contractors who planned infiltrations, searched for vulnerabilities, and remained undetected within the adversary's system for months.

Even the most sophisticated operations still followed human rhythms, relied on human judgement, and faced human limitations.

In 2026, that model is rapidly disappearing.

Today, the most dangerous offensive cyber operations are increasingly led not by operatives, but by autonomous AI systems capable of independently identifying targets, adapting malware, exploiting vulnerabilities, and making decisions in real time without direct human control.

The pace of conflict has become faster than people can keep up with. In some sectors, the time between the detection of a threat and the complete compromise of a system is measured in seconds.

This is changing the nature of cyber conflict. The digital space is no longer limited to data theft or adversary surveillance.

The focus is now on infrastructure, energy, financial systems, logistics, telecommunications, and the state's ability to function under the pressure of autonomous digital attacks.

Cyberspace is no longer an auxiliary front in modern conflicts; it has become the central arena of strategic competition between states.

Malware that changes as you watch it

Traditional antivirus systems relied on pattern recognition. Malware was identified by comparing it with known signatures and previously recorded malware behaviour. This approach is becoming increasingly difficult to use today.

A new generation of AI-powered malware can alter its own code in real time to evade detection. In the first half of 2026, attacks were recorded in which malware changed its cryptographic signature every few seconds, making it virtually undetectable by standard protection systems.

This means that traditional protection models are losing the advantage they have held for years. Systems that depend on recognising known patterns now lag behind attacks that change faster than they can be detected.

> Smaller states, proxy actors and criminal networks can now wield capabilities that until recently were reserved for only the largest intelligence powers

For this reason, some cyber security experts are increasingly using terms from biology rather than computer science. Modern malware behaves more like an evolving virus than a traditional software tool.

The consequences are also serious at the geopolitical level. Developing sophisticated offensive malware once required large budgets, elite teams and years of work. Artificial intelligence significantly lowers the barrier to entry.

Smaller states, proxy actors and criminal networks can now wield capabilities that until recently were reserved for only the largest intelligence powers. The monopoly over advanced cyber capabilities is beginning to weaken.

The end of the "bad phishing" era

For years, phishing campaigns had one major weakness: the human behind the keyboard. Grammatical errors, poor translation,

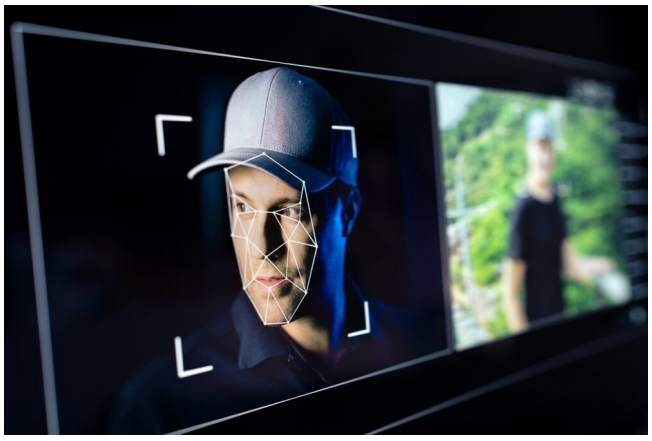
unconvincing tone, or cultural inconsistencies often exposed fraud attempts before an attack could succeed. Artificial intelligence has virtually eliminated this problem.

Offensive LLM models now generate millions of hyper-personalised messages that precisely mimic companies' communication styles, executive writing styles and internal corporate language.

Attacks no longer resemble generic scams; they appear to be legitimate business communications.

This is particularly dangerous because most serious compromises still begin with the manipulation of trust rather than a technical breach of the system.

However, a genuine qualitative shift occurred with the development of the so-called Deep-Live operation. These are real-time video calls in which AI fully simulates the face, voice, facial expressions, and communication style of a specific person.



In 2026, there was an increase in attacks where financial transfers were authorised following fake video meetings with company "directors" who never actually participated in the conversation

In 2026, there was an increase in attacks where financial transfers were authorised following fake video meetings with company "directors" who never actually participated in the conversation.

The goal of these operations is no longer merely to steal passwords or access data. Attackers attempt to manipulate the decision-making process within organisations directly, using legitimate communication channels.

This is a much more serious problem than traditional cyber fraud. Modern institutions operate on the assumption that it is possible to trust the identity of the interlocutor.

When AI becomes capable of mass identity falsification in real time, one of the fundamental mechanisms of trust in digital society collapses.

In practice, organisations are entering a period when it will no longer be sufficient to check who sent the message. They will have to verify whether the person on the other end of the video call actually exists.

AI has eliminated reaction time

Even two years ago, discovering a serious software vulnerability required months of work by leading experts in reverse engineering and code analysis. Today, this work is increasingly performed by AI clusters.

Models trained on large public and private codebases can identify logic flaws, unsafe dependencies, and architectural errors within minutes of a new software version or security patch being released.

This dramatically changes the relationship between attackers and defenders.

> Power grids, transport systems, and industrial plants often cannot implement patches immediately without risking their own operation

Traditional cyber protection relied on the assumption that there was a window of time between the announcement of a vulnerability and its mass exploitation. IT teams expected to have days or weeks to react, install patches,

and reorganise systems.

That window is rapidly shrinking.

With critical infrastructure, the situation is even more dangerous. Power grids, transport systems, and industrial plants often cannot implement patches immediately without risking their own operation. Autonomous AI systems exploit this very slowness as their main point of attack.

The problem is no longer solely technological. It is now the institutional slowness of states and companies that attempt to respond to threats at the pace of bureaucratic procedures, while autonomous systems operate at the speed of machine reaction.

The great powers no longer have a monopoly

The most significant strategic change may not be the technology itself, but that it has made offensive cyber operations widely accessible.

In the previous decade, only a few states had the capacity to conduct serious cyber-kinetic operations against an adversary's critical infrastructure. Today, the situation is changing rapidly.

Offensive AI tools are emerging on dark web markets as much more advanced successors to earlier models such as WormGPT. Attackers no longer need to be expert programmers; access to a suitable AI system and basic operational knowledge is sufficient.

> Autonomous offensive systems are optimised for efficiency and speed, not political rationality or controlled escalation

This creates opportunities for a new type of asymmetric conflict. Smaller states, regional actors, and proxy networks can now inflict serious damage on adversaries with much larger military budgets. Operations targeting energy infrastructure, water supply, and logistics systems are of particular concern.

Security assessments from the first half of 2026 increasingly warn of scenarios in which AI autonomously analyses network traffic, maps system dependencies, and independently identifies the most critical points for infrastructure paralysis.

This introduces an entirely different logic of escalation. Traditional military conflicts involved a certain degree of political control over the pace of conflict. Autonomous offensive systems are optimised for efficiency and speed, not political rationality or controlled escalation.

This is exactly where the greatest risk lies.

AI vs AI war

Defence systems attempt to respond using the same logic – automation.

Modern SOC centres no longer operate on a model where an analyst receives an alert and then manually decides on a response.

AI systems now autonomously isolate parts of the network, block traffic, and shut down compromised segments of infrastructure without waiting for human confirmation.

It is no longer a question of efficiency, but of system survival. Human reactions are simply not fast enough for a conflict between autonomous digital systems. However, this is precisely where a new problem arises.

> Future major digital crises may arise not only from a successful attack but also from an overactive autonomous defence response

Security experts increasingly warn about the possibility of so-called algorithmic escalations – situations in which offensive and defensive AI systems engage in a chain of accelerated

reactions that can cause mass disruption without either party intending such consequences.

In theory, a localised compromise attempt could trigger autonomous defence mechanisms, shutting down entire segments of a nation's digital infrastructure as a precaution.

Future major digital crises may arise not only from a successful attack but also from an overactive autonomous defence response. For such scenarios, most countries still lack both a legal and an operational response.

The new reality: paralysis without a shot being fired

For many governments, cybersecurity is still considered the responsibility of technical teams. In reality, it is already a matter of national resilience and political stability.

Autonomous AI operations are transforming cyberspace from a domain of espionage to one of infrastructure warfare.

Digital infrastructure has become a central vulnerability for states

The objective is no longer merely to steal data or monitor adversaries; it is now the functional paralysis of society.

A modern state today does not need to be bombed to be destabilised. Interruptions in payment transactions, a decline in telecommunications, a collapse of logistics, shutdowns of energy systems, or disruption of hospital operations are sufficient. All this can be done remotely, continuously, and with a high degree of deniability.

That is precisely why the year 2026 represents an important moment for global security. Digital infrastructure has become a central vulnerability for states, and autonomous artificial intelligence is, for the first time, enabling mass offensive operations at speeds that exceed human control.

The greatest weakness of states is no longer a lack of technology. The problem is that autonomous systems are evolving much faster than the political and security structures attempting to control them.