July 2026

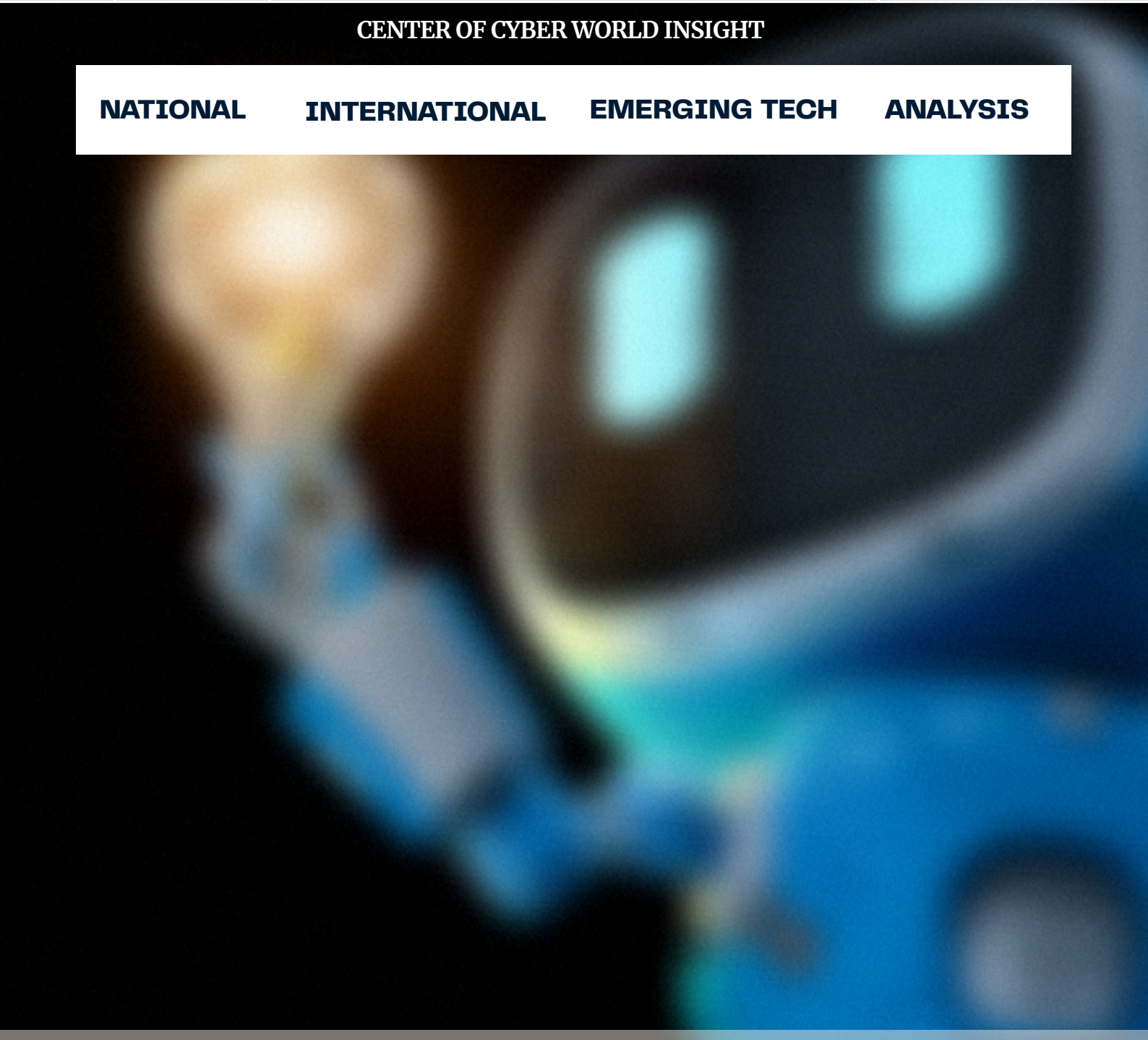
CYBER WATCH

CYBER WORLD INSIGHT

VOLUME. 02, ISSUE 14

CENTER OF CYBER WORLD INSIGHT

NATIONAL INTERNATIONAL EMERGING TECH ANALYSIS



WHERE CYBERSECURITY MEETS INNOVATION

ISSUE 14 | VOL 2 | JULY 26

July 2026

CYBER WATCH

VOLUME. 02, ISSUE 14

CENTER OF CYBER WORLD INSIGHT

July 01-15th, 2026

About

CyberWatch is a policy and op-ed e-paper dedicated to exploring how technology is transforming Pakistan's society, economy, and governance. We bring together voices from academia, industry, and policy to debate the opportunities and risks of the digital age. Our mission is to inform, challenge, and shape the national conversation on Pakistan's technological future.

Publishing Information

Center for Cyber Research and Artificial Intelligence (CCRAI)©2023–2025
The Center for Cyber Research and Artificial Intelligence Pakistan
Office #401, Omega Heights, E/11-3,
Islamabad, Pakistan
🌐 Website: www.ccrai.org.pk
📧 Email:
news@cyberworldinsight.com
📱 Phone/WhatsApp: +92 333 5221408

Digital Edition

This is the Fortnightly Digital Edition of Cyber Watch.
📲 Available online at:
🌐 www.cyberworldinsight.com/cyberwatch
📥 Downloadable in PDF format for offline reading.

Design Team

Lead Designer:
- Kainat Shahid

Editorial Team

- Urwa Urooj
- Mehrosh Khan
- Fizza Muhammad

Contributors

- Hadia Sarwar
- Ayesha Asif
- HIba Tanveer
- Anzilah Ahmad

July 2026

CYBER WATCH

VOLUME. 02, ISSUE 14

CENTER OF CYBER WORLD INSIGHT

July 01st-15th, 2026

FROM THE TEAM

Cybersecurity, artificial intelligence, and emerging technologies continue to redefine the global digital landscape. As cyber threats become more sophisticated and AI accelerates both innovation and risk, governments, businesses, and institutions are placing greater emphasis on digital resilience, secure infrastructure, and responsible technological advancement.

Beyond reporting the latest developments, this edition seeks to provide context, analysis, and practical insights into the evolving intersection of cybersecurity, artificial intelligence, technology, and international affairs. As digital transformation accelerates, understanding both the opportunities and the challenges of emerging technologies has never been more important.

We hope this issue offers our readers valuable perspectives on the rapidly changing cyber domain and contributes to informed discussions on building a safer, more resilient digital future.

Finally, we extend our sincere appreciation to our contributors, editorial team, and readers for their continued support and commitment to advancing cybersecurity awareness and knowledge.

Editor-in-Charge, CyberWatch E-paper,
Center for Cyber World Insight

Kainat Shahid

July 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 14

India Approves Buying $5.46 Billion in Military Equipment

The approval by India of a massive acquisition of military hardware clearly indicates that the country continues to prioritize defence build-up efforts. The procurement process is consistent with India's long-term policy aimed at the modernization of its military forces due to the presence of security challenges associated with China and Pakistan.

In terms of strategic considerations, the initiative can be considered an attempt to strengthen the country's deterrence capabilities, increase technological advancement, and enhance India's influence within the region. However, there are also fears about the possible regional arms race.

With respect to Pakistan's viewpoint, India's increase in its military capabilities can be considered an imbalance in the regional balance of power. This could lead to a security dilemma, wherein a nation's defensive actions would be seen as offensive by the other side.

Apart from that, a valid question is raised about the priorities of a nation when huge amounts of money are being spent on the military despite numerous socio-economic problems. While the government needs to safeguard the country, such spending could also result in neglecting health, education, poverty, and the economy.

(Source: Dawn, 2026)

July 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 14

US Must Recognise 'Realities Have Changed' After War, Says Iran's Ghalibaf

Mohammad Bagher Ghalibaf, Speaker of the Iranian Parliament, has stated that the United States must recognise that "realities have changed" following the recent military confrontation. According to Iran, the latest developments have strengthened the country's bargaining position and altered the regional strategic landscape. Speaking during a meeting with Uzbekistan's parliamentary speaker, Ghalibaf stated that post-war developments had compelled Washington to acknowledge the changing realities in the region. He also expressed hope that these developments could create favourable conditions for expanding trade relations and eventually contribute to the easing of sanctions.

From a political perspective, the statement reflects Iran's effort to project confidence and resilience while reinforcing national cohesion. It also conveys Tehran's expectation that future diplomatic engagements should acknowledge the changing geopolitical environment created by the recent conflict.

(Source: Dawn , 2026)

July 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 14

MEDIATORS SAY 'POSITIVE PROGRESS' MADE IN US–IRAN TALKS IN DOHA

Mediators have reported "positive progress" in the ongoing talks between the United States and Iran in Doha, signalling a constructive step towards diplomatic engagement despite continuing regional tensions.

According to officials, both sides agreed to continue discussions, with another round of negotiations expected after the conclusion of Iran's national mourning period. The negotiations reportedly focused on confidence-building measures and maintaining communication channels between the two parties.

Although no major breakthrough has been announced, the discussions demonstrate the continued importance of dialogue in addressing longstanding political differences. The reported progress highlights diplomacy as an essential mechanism for conflict management and regional stability amid an evolving international security environment.

(Source: Associated Press (AP), 2026)

WSIS FORUM 2026

6-10 July 2026
Geneva, Switzerland

The World Summit on the Information Society (WSIS+20) celebrates twenty years of global work toward an inclusive, secure and development-oriented digital society. The conference brings together both governments and other stakeholders, including international organizations, the private sector, academia, and civil society, to collectively define the agenda for digital governance. The summit is organized by the International Telecommunication Union (ITU) and co-organized by UNESCO, UNDP, and UNCTAD and takes place in Geneva.

The forum targets issues of the digital age, most of which are of critical importance, including artificial intelligence, cyber security, digital public infrastructure, universal connectivity, digital inclusion and bridging the global digital divide. It also offers a platform for policy discussions and experts to share insights on new challenges, including online safety, misinformation, data governance, and responsible use of frontier technologies.The 2026 forum is of particular importance because it is the first forum to be convened since the UN General Assembly's WSIS+20 Review, which reconfirmed global commitments to expanding the cooperation in the digital domain and adopting the WSIS Action Lines.

The event features high-level ministerial dialogues, policy discussions, thematic exhibitions, youth engagement initiatives, and the annual WSIS Prizes, showcasing innovative digital projects from around the world.WSIS offers a valuable opportunity for countries such as Pakistan to enhance collaboration with global partners, share strategies for digital governance, and highlight national initiatives in areas like AI, cybersecurity, and digital transformation. The forum will continue to be one of the most powerful forums to advance inclusive, secure, and sustainable digital development as digital technologies continue to transform economies and societies.

July 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 14

PAKISTAN'S DEVELOPMENT OF AN ADVANCED CYBERSECURITY FRAMEWORK

The Government of Pakistan has proposed an advanced cybersecurity framework that will apply to government organizations hosting their websites and digital applications abroad. Under this framework, government data will be transferred to secure data centres located within Pakistan. This proposal is an important part of the Pakistan Information Security Framework (PISF).

The framework outlines several measures to strengthen the security of Pakistan's government digital infrastructure. To meet mandatory cybersecurity standards, government organizations will be required to operate secure data centres, email services, and web-hosting platforms within the country. They must also implement robust network security measures, including next-generation firewalls, intrusion detection and prevention systems (IDPS), Distributed Denial-of-Service (DDoS) protection, secure backup mechanisms, vulnerability management, continuous monitoring through Security Operations Centres (SOC), Security Information and Event Management (SIEM) systems, and regular third-party security audits.

In addition, organizations will be required to adopt advanced authentication methods for websites, along with email archiving and backup capabilities. The framework also recommends protection against advanced persistent threats (APTs) and the implementation of domain authentication protocols, including SPF, DKIM, and DMARC, to improve the security and integrity of government email systems.

These measures reflect Pakistan's broader efforts to strengthen cyber resilience, safeguard sensitive government data, and establish a secure digital ecosystem for public-sector institutions.

(Source: SAMAA News , 2026)

July 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 14

Pakistan Expands AI Diplomacy and Digital Skills Development

Federal Minister for Information Technology and Telecommunication Shaza Fatima Khawaja held bilateral meetings with Sri Lankan and Egyptian officials on the sidelines of the World Summit on the Information Society (WSIS) in Geneva to strengthen cooperation in digital governance and emerging technologies. During her meeting with Dr. Hans Wijayasuriya, Chief Adviser to the President of Sri Lanka on the Digital Economy, both sides discussed cooperation in information technology, the promotion of the digital economy, and e-governance. Discussions on Artificial Intelligence (AI) sovereignty were also held, while Pakistan's IT exports to Sri Lanka, which stood at US$424,000 during the fiscal year 2024, were highlighted as an area with significant growth potential. Both countries agreed to enhance collaboration in the IT sector and share best practices.

The Federal Minister also met Mahmoud Badawi, Deputy Minister for Digital Transformation of the Arab Republic of Egypt. The two sides agreed to strengthen cooperation in information technology, telecommunications, and digital governance during discussions held on the sidelines of the United Nations Global Dialogue on AI Governance. Highlighting Pakistan's domestic initiatives, the Minister stressed that technical skills are essential for learning and regulating AI. She emphasized that AI literacy has become increasingly important for both technical professionals and non-technical workers. The programme, implemented in collaboration with global partners including Google, aims to strengthen Pakistan's digital workforce and accelerate the country's transition towards an AI-driven economy.

(Source: AP, 2026)

July 2026

TECHNOLOGY SPOTLIGHT

VOLUME. 02, ISSUE 14

Siemens Xcelerator: Powering the Next Generation of Digital Twins

Industrial digital transformation drives Siemens Xcelerator to become one of the world's premier platforms for the development and management of Digital Twins. Xcelerator, introduced by Siemens in 2022, is an open digital business platform that brings together industrial software, IoT connected hardware, cloud services, and artificial intelligence to ensure real-time virtual representations of physical assets and systems. It is not a single application, but rather an ecosystem that empowers organizations to design, simulate, monitor and optimize products, factories, buildings and critical infrastructure across their lifecycle.

The Digital Twin is one of the standout features of Xcelerator. These systems combine real-time sensor data with engineering models and AI-driven analytics, enabling organizations to anticipate equipment failures, simulate operational scenarios prior to deployment, minimize downtime, optimize energy usage, and make quicker informed decisions. From manufacturing and transportation to smart city development and healthcare and utilities, the platform can be used by industries to optimise existing facilities and new infrastructure projects.

July 2026

VOLUME. 02, ISSUE 14

TECHNOLOGY SPOTLIGHT

Technology Focus
Digital Twins, Industrial AI, IoT, Industrial Software, Cloud Services

Deployment
Cloud-based and Hybrid

Core Components
Software, IoT-enabled hardware, digital services, partner ecosystem, digital marketplace

Primary Applications
Smart Cities, Manufacturing, Buildings, Energy, Transportation, Healthcare

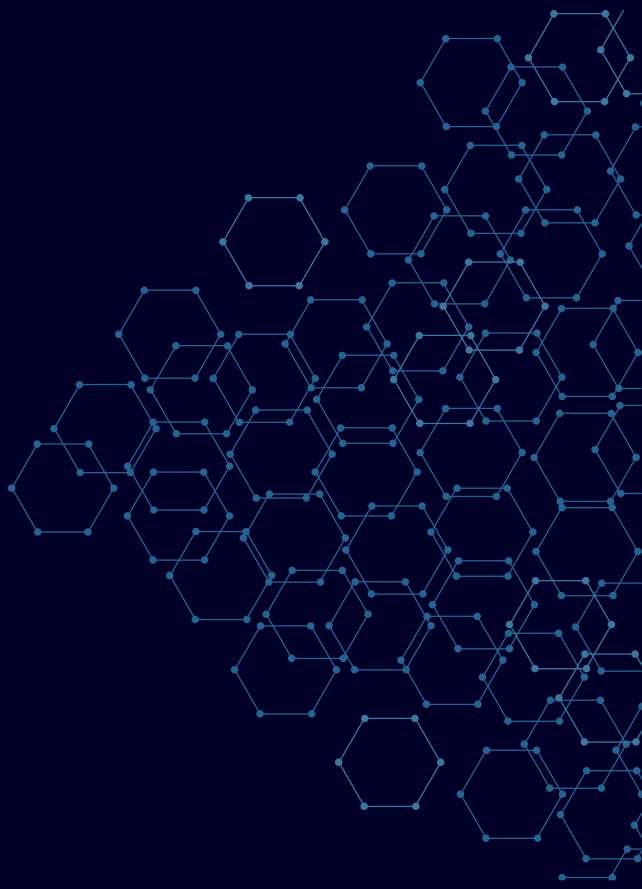
Supporting Technologies
Artificial Intelligence, Internet of Things (IoT), Edge Computing, Cloud Computing, Data Analytics

Key Capability
Creates comprehensive Digital Twins for products, infrastructure, factories, and operational systems

Target Users
Governments, industries, infrastructure operators, manufacturers, utilities, smart city developers

Notable Partnerships
NVIDIA, Microsoft, and a growing ecosystem of certified technology partners

Business Model
Open ecosystem with interoperable software, hardware, and digital services



July 2026

AI ACROSS DISCIPLINES

VOLUME. 02, ISSUE 14

How Password Managers Work?

BY HIBA TANVEER

As cyber threats are increasing day by day, we need stronger passwords to protect our personal information. We all have online accounts, but remembering their passwords is difficult. Therefore we need a solution to this problem. For this, we use password managers. They are secure, convenient, and easy to manage.

A password manager is software designed to store passwords in a digital vault. There is a need to remember only one master password. The other passwords are automatically saved by the password manager.

How Do Password Managers Work?

Password managers store passwords in end-to-end encrypted vaults. These vaults can store multiple passwords at once, while you need to remember only one master password. It is very important not to forget the master password; otherwise, you may lose access to the passwords stored by the password manager. In such a case, you need to reset all your passwords.

To avoid this, always keep a face or fingerprint password as a backup. Password managers also help identify weak passwords, as they can become vulnerable to phishing attacks. Therefore, they alert you so that you can surf safely online.

Benefits of Using a Password Manager

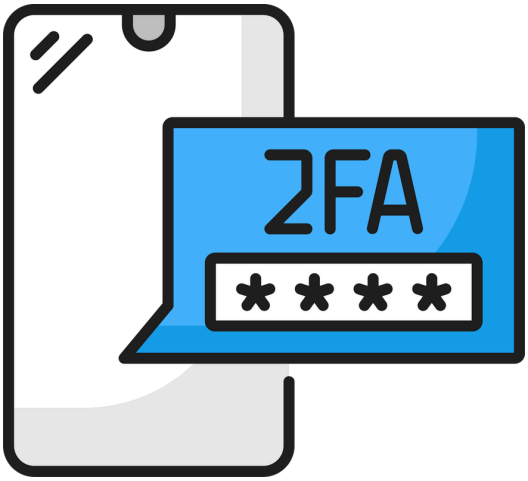
A password manager has many benefits, such as:

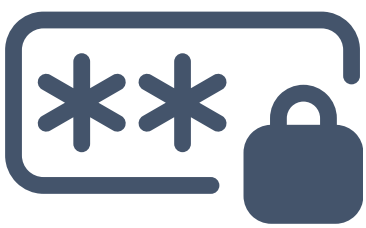
- *Security:* It provides online security and prevents criminals from stealing data from your websites. Moreover, it can generate random passwords to provide strong security.
- *Saves Time*: It saves time by keeping you logged in, as it has saved your passwords. Therefore, there is no need to re-enter your passwords repeatedly.
- *Autofill Feature*: It has a user-friendly autofill feature. Instead of entering your information again, it automatically fills it.
- *Same Passcode for Multiple Devices*: You can log in from multiple devices using the same password.
- *Easy Change of Passwords*: You can easily change your passwords. If your online account gets hacked, you can change your password with the help of a password manager.

Conclusion

In an era where cyber threats are common, it is not a good decision to rely on repeated passcodes. Password managers offer strong and reliable passwords and can save multiple passwords in encrypted vaults. They are an effective way to guard your data from hackers online.

Password managers also have many useful features, such as improved security, reduced password reuse, time-saving functionality, and much more. By trusting a good password manager, you can safeguard your data and confidential information from criminals online.





July 2026

ANALYSIS

VOLUME. 02, ISSUE 14

NATO CYBER DEFENCE DOCTRINE UPDATE: HOW THE NEW FRAMEWORK IS RESHAPING INTERNATIONAL AFFAIRS

BY ANZILAH AHMAD

Introduction

Cyberspace has become the newest battlefield of the twenty-first century. Unlike conventional warfare, cyber warfare can cross borders instantly, disrupt critical infrastructure, manipulate public opinion, and threaten national security without a single soldier crossing a frontier. Governments, militaries, financial institutions, healthcare systems, and energy networks now depend heavily on digital technologies, making cyber resilience a strategic necessity rather than a technical option.

Recognizing these evolving threats, the North Atlantic Treaty Organization has significantly updated its cyber defence doctrine. While NATO originally focused on protecting military communication networks, its modern cyber strategy now integrates military, political, technical, and civilian capabilities into a unified framework. The Alliance considers cyberspace an operational domain alongside land, air, sea, and space, reflecting the reality that modern conflicts increasingly begin with digital attacks rather than conventional weapons.

The latest reforms, introduced through the 2023 Vilnius Summit and strengthened at the 2024 Washington Summit, represent one of the most comprehensive transformations in NATO's cyber posture since the Alliance was established in 1949. These updates emphasize resilience, intelligence sharing, collective defense, protection of critical infrastructure, and closer cooperation with governments and industry.

The Evolution of NATO's Cyber Defense Doctrine

For decades after its creation, NATO concentrated primarily on conventional military threats during the Cold War. Cybersecurity received limited

attention because digital infrastructure had not yet become central to national defense.

Several important developments define this new framework.

1. **Enhanced Cyber Defense Pledge**

Originally adopted in 2016, the Cyber Defense Pledge required member states to improve national cyber capabilities.

At the 2023 Vilnius Summit, NATO strengthened this commitment by introducing more ambitious national goals. Member countries agreed to improve cyber resilience, particularly for critical infrastructure such as electricity grids, transportation systems, telecommunications, healthcare, banking, and emergency services.

2. **Virtual Cyber Incident Support Capability (VCISC)**

One of NATO's most innovative initiatives is the Virtual Cyber Incident Support Capability (VCISC).

Instead of waiting for lengthy diplomatic coordination after a cyberattack, the VCISC enables experts from across NATO to provide rapid technical assistance to affected member states during significant cyber incidents.

This capability enhances:

- Faster incident response
- Technical coordination
- Intelligence sharing
- Recovery support
- Cross-border cooperation

The VCISC reflects the understanding that cyberattacks often spread across multiple countries within minutes.

3. **NATO Integrated Cyber Defense Centre**

Perhaps the most significant reform announced at the 2024 Washington Summit is the establishment of the NATO Integrated Cyber Defense Centre (NICC) at SHAPE in Belgium.

The Centre brings together:

- Military cyber specialists
- Civilian experts
- Intelligence professionals
- Industry partners.
- Technology researchers

Its objectives include improving situational awareness, strengthening network protection, identifying emerging cyber threats, and coordinating cyber operations across the Alliance. The Centre also enhances cooperation with privately owned critical infrastructure operators, recognizing that many essential services are run by the private sector.

Why These Changes Matter?

The updated doctrine signals a fundamental transformation in international security.

For decades, military power was measured by the size of armies, navies, and air forces. Today, a country's cyber capabilities increasingly determine its ability to defend itself.

Cyberattacks can disrupt power grids, disable hospitals, interrupt financial markets, influence democratic elections, and undermine public trust all without conventional military engagement.

By integrating cyber defense into its overall deterrence strategy, NATO aims to convince potential adversaries that malicious cyber activities will face coordinated political, technical, diplomatic, and, where appropriate, collective responses. This strengthens deterrence while reducing the likelihood of successful cyber aggression

Impact on International Affairs

The updated NATO cyber defense doctrine is influencing international affairs in ways that extend far beyond the military. Today, cybersecurity is closely linked to diplomacy, economic stability, intelligence sharing, and national resilience. Governments increasingly recognize that cyberattacks can have strategic consequences comparable to conventional military actions.

Cyber Deterrence in a New Era

Traditional deterrence relied on military strength and nuclear capability. NATO's updated doctrine introduces a broader concept of cyber deterrence, which seeks to discourage cyberattacks by improving resilience, enhancing intelligence sharing, and demonstrating that allies will respond

collectively to serious cyber incidents. The doctrine emphasizes prevention, rapid response, and coordinated defense rather than relying solely on retaliation.

Strengthening International Cooperation

Cyber threats ignore national borders, making international cooperation essential. NATO now works more closely with the European Union, partner countries, private technology companies, and cybersecurity research institutions. Information sharing has become a central pillar of the Alliance's strategy because attackers often target several countries simultaneously. The creation of the NATO Integrated Cyber Defense Centre (NICC) will further improve situational awareness by bringing together military experts, intelligence specialists, and technical professionals to detect and respond to cyber threats more effectively.

Real-World Case Studies

1. ***Estonia (2007)***

The cyberattacks against Estonia marked one of the world's first large-scale cyber campaigns against a nation-state. Government websites, banks, media organizations, and communication services were disrupted through coordinated Distributed Denial-of-Service (DDoS) attacks.

Although there were no physical casualties, the incident demonstrated that digital attacks could paralyze essential services and undermine public confidence. The attack became a turning point in NATO's cyber policy and eventually led to the establishment of the NATO Cooperative Cyber Defense Centre of Excellence in Tallinn.

2. ***WannaCry Ransomware (2017)***

The WannaCry ransomware attack spread across more than 150 countries, infecting over 230,000 computers within days. Hospitals, businesses, transportation systems, and government agencies experienced major disruptions.

The attack highlighted how vulnerabilities in widely used software could rapidly become global security issues, reinforcing the importance of international cyber cooperation.

3. ***NotPetya (2017)***

Originally targeting organizations in Ukraine, NotPetya quickly spread worldwide. Major multinational companies suffered severe operational disruptions, with estimated global damages exceeding US$10 billion.

Unlike ordinary cybercrime, NotPetya demonstrated that cyber operations could generate economic losses comparable to those caused by major natural disasters.

4. ***Russia–Ukraine Cyber Conflict***

Since the beginning of Russia's full-scale invasion of Ukraine in 2022, cyber operations have accompanied conventional military action. Malware, satellite communication disruptions, phishing campaigns, and attacks on government services have become regular features of the conflict.

These events have reinforced NATO's view that cyberspace is now a permanent operational domain requiring continuous preparedness.

Implications for International Affairs

NATO's updated cyber doctrine is reshaping global politics in several important ways: Cybersecurity is now a central element of national security strategies. Collective defense extends into cyberspace, where major attacks may trigger coordinated responses. Public–private partnerships are becoming increasingly important because much critical infrastructure is owned by private companies. International law and diplomacy are adapting to address cyber conflict, attribution, and state responsibility. Emerging technologies, including artificial intelligence, quantum computing, and autonomous systems, are becoming integral to cyber defense planning.

As a result, cyber capability is no longer viewed simply as an IT function—it has become a measure of geopolitical influence and national resilience. NATO's evolving framework reflects this transformation and is likely to shape international security policy for years to come.

Challenges Facing NATO's Cyber Defence Strategy

Despite major improvements, NATO's updated cyber defence doctrine faces several significant challenges.

1. ***Attribution of Cyberattacks***

One of the greatest difficulties in cyberspace is identifying the real attacker. Cybercriminals and state-sponsored groups often hide their identities by routing attacks through multiple countries or compromised systems. This makes it difficult to determine who is responsible and whether a cyberattack should trigger a collective response under NATO's security commitments.

2. ***Rapid Technological Change***

Emerging technologies such as Artificial Intelligence (AI), Quantum Computing, the Internet of Things (IoT), and 5G/6G networks are creating new opportunities but also expanding the cyber threat landscape. NATO must continuously adapt its capabilities to address these evolving risks.

3. ***Protection of Critical Infrastructure***

Most critical infrastructure, including electricity, banking, healthcare, telecommunications, and transportation, is operated by private companies rather than governments. Effective cyber defence therefore requires strong public-private partnerships, information sharing, and coordinated incident response.

4. ***Differences Among Member States***

NATO's 32 member countries have varying levels of cyber capability, financial resources, and technical expertise. While some nations possess highly advanced cyber forces, others continue developing their digital resilience. Ensuring consistent standards across the Alliance remains a major challenge.

Future Outlook

The future of cyber defense will depend on cooperation, innovation, and adaptability. NATO is expected to invest further in artificial intelligence for real-time threat detection. Quantum-resistant encryption to prepare for future computing advances. Cyber exercises and simulations involving military and civilian partners. Protection of undersea communication cables, satellites, and cloud infrastructure. Enhanced collaboration with universities, research institutions, and technology companies. The Alliance is also likely to deepen partnerships with international organizations and like-minded countries to improve global cyber resilience.

Conclusion

Cybersecurity has become one of the defining security challenges of the twenty-first century. As societies become increasingly digital, cyberattacks have the potential to disrupt economies, influence politics, and threaten international peace without traditional military confrontation.

NATO's updated cyber defense doctrine represents a significant evolution in collective security. By strengthening resilience, improving cooperation, integrating cyber capabilities into military planning, and establishing institutions such as the NATO Integrated Cyber Defense Centre, the Alliance has positioned itself to address the growing complexity of digital conflict. However, technology continues to evolve faster than policy. Artificial intelligence, quantum computing, ransomware, and hybrid warfare will require continuous adaptation, international cooperation, and sustained investment.

Ultimately, NATO's new cyber defense framework is more than a military strategy. It is a blueprint for safeguarding democratic societies in the digital age. Its success will depend not only on technological capability but also on trust, collaboration, and a shared commitment to maintaining a secure, open, and stable cyberspace.

July 2026

AI ACROSS DISCIPLINES

VOLUME. 02, ISSUE 14

AI Agents in Smart Cities: Establishing Tomorrow Through Intelligent Innovation

BY HADIA SARWAR

As cities are expanding, so do the problems and challenges of maintaining transportation, security, civil services, and medical care. Traditional and old networks may face challenges in keeping up with the increasing population and expanding demands, and this is exactly where Artificial Intelligence (AI) agents are creating a huge and meaningful difference. Instead of replacing humans, these intelligent networks are helping cities become more consistent, streamlined, and resourceful.

What Are AI Agents?

In the context of generative artificial intelligence, AI agents are a class of intelligent agents that can pursue goals, use tools, and take actions with varying degrees of autonomy.

Unlike simple automation, AI agents can adapt to changing situations and refine their performance over time.

Expansion of Smart Cities

A smart city uses digital technologies and linked devices to improve the quality of life for its residents. These technologies collect and analyse data to improve decision-making across civil services. AI agents play the role of intelligence behind several sectors and systems, allowing cities to respond faster and work more efficiently.

Today, smart cities are not just a vision of the future. Around the world, governments are investing billions in AI-powered improvements for the betterment of economic growth.

Why Are AI Agents Important in Smart Cities?

1. ***Improved Public Safety***

AI-powered systems can detect unusual activities and identify emergencies more quickly and efficiently. They can also alert the authorities in real time during accidents and natural disasters. These AI-powered systems can support emergency services, respond more efficiently, and help save many lives.

2. ***Efficient Management of Waste***

Like today, waste is collected at fixed times. By using AI agent monitors on smart bins, sensors can indicate which bins and areas need to be cleaned. This can optimise fuel consumption, reduce vehicle costs, and minimise the wastage of time.

3. ***Modern Healthcare Systems***

By modernising healthcare services in smart cities, AI-powered systems can analyse medical reports, assist doctors, prepare patient prescriptions, and manage hospital patient availability. By using these technologies, healthcare professionals can improve their focus on patients. Reducing the burden of preparing reports and performing other administrative work allows doctors to devote more attention to patient care.

4. ***Citizen Assistance***

These AI agents are helping citizens access government services, report their issues, use online banking facilities, and pay their bills. Moreover, they can receive assistance 24/7 whenever they need it.

Looking Forward

The future of smart cities will depend on successful cooperation and understanding between humans and technology. AI agents are powerful tools, but their true value lies in supporting human decision-making rather than replacing it.

SIGNING OFF..

UNTIL WE DEFEND AGAIN

Stay ahead of every threat

Subscribe for exclusive insights, expert analysis, and real time updates on the evolving cybersecurity landscape

@cyberworldinsight