Editorial

Considerations Concerning Cybersecurity Evolutions in International Context

Professor Emeritus Ioan C. BACIVAROV, PhD
EUROQUALROM - Faculty of Electronics, Telecommunications, and Information Technology, National University of Science and Technology POLITEHNICA Bucharest, Romania
President of Romanian Association for Information Security Assurance (RAISA)

1. *Cybersecurity* or *Information Technology security (IT security)* is the protection of computer systems and networks from attack by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide. These *cyberattacks* are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes.

Cybersecurity is one of the most significant challenges of the contemporary world, due to both the complexity of information systems and the societies they support. *Security* is of especially high importance for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance.

Today we are all aware of the importance of the *IT security field*, as well as its role in the smooth development of all human activity.

2. Based on the international context, *cybersecurity* has evolved from a *technical IT issue* into a *critical component* of national security, economic stability, and international relations. The current landscape is characterized by increasing geopolitical fragmentation, the rise of state-sponsored threats, and a widening technological divide. We mention here - based on the analysis of several bibliographical sources - some *key perspectives on cybersecurity from an international viewpoint:*

A*. *Geopolitical Fragmentation and Digital Sovereignty

- *Competing Models:* A major divide exists between a "free and open internet" model favored by liberal democracies and a "digital sovereignty" model supported by nations like China and Russia, which emphasizes state control over digital infrastructure.
- *Mercantilism and Security*: There is a return to a "regulatory mercantilism" where trade and economic security are indistinguishable from cyber security.

Nations are focusing on regionalizing supply chains, especially in critical technology like semiconductors.
- *Hybrid Warfare:* Cyber capabilities are routinely used for espionage and sabotage, blurring the line between peace and conflict.

B. *Evolving Threat Landscape*
- *Ransomware-as-a-Service (RaaS):* Ransomware has become the primary tool for monetizing cybercrime, with massive campaigns like WannaCry affecting over 150 countries.
- *Supply Chain Vulnerabilities***:** Supply chain attacks, such as SolarWinds, are a major concern, with 54% of large organizations identifying third-party risks as a top challenge.
- *Artificial Intelligence in Warfare***:** Artificial Intelligence (AI) is accelerating the conflict, acting as a force multiplier for both automated defense and sophisticated, deceptive attacks.

C. International Cooperation and Regulatory Frameworks
- *Regional Dominance (EU/US):* The European Union has adopted a strong regulatory approach with GDPR and the NIS Directive, which influences global standards, often described as the "Brussels Effect".
- *Standardization Challenges***:** While organizations like NIST and ISO offer global frameworks, national differences in law enforcement and data privacy make uniform, binding international cyber laws difficult to enforce.
- *Public-Private Partnerships (PPPs):* Given that the private sector owns most critical infrastructure, international consensus emphasizes that governments must partner with tech companies for threat intelligence sharing.

D. *The Global North-South Divide*
- *Capacity Disparities***:** The COVID-19 pandemic highlighted a significant cyber-capacity gap between the Global North and South, particularly in infrastructure, data collection, and threat reporting.
- *Dependency Risks***:** Developing nations often face or are forced to create cybersecurity dependencies on technology giants based in the US or China.

E. *Emerging Trends and Priorities*
- *Workforce Shortage***:** Some experts estimate a global shortage of 3.5 million cybersecurity professionals.
- *Internet of Things Security***:** With billions of new connected devices, securing the Internet of Things (IoT) is now crucial to preventing them from being used in massive, cascading botnet attacks.
- *Data Protection & Privacy***:** Over 160 countries now have legislation regarding personal data protection, with a strong, rising global focus on enforcing privacy rights.

3. As of June 2026, cybersecurity is in a state of *perpetual cyber conflict,* driven by AI adoption, geopolitical fragmentation, and state-sponsored operations acting below the threshold of traditional war. Conflicts, including Russia-Ukraine and Middle East

tensions, have rendered cyber operations an inseparable part of modern hybrid warfare, prioritizing "access-first" infiltration of critical infrastructure and disinformation campaigns.

We can mention some *actual* ***International Context Drivers***:

- *Persistent Conflict Drivers*: Russia-Ukraine continues as a template for cyber-kinetic integration. Middle Eastern conflicts have prompted retaliation attacks on Western critical infrastructure, as reported by *ECCU.edu*.
- *Geopolitical Fragmentation:* The world is splitting into two technological spheres (US/Western vs. China-aligned), leading to incompatible tech standards, data regulations, and heightened supply-chain security risks, notes the *World Economic Forum*.
- "*Access-First" Strategy*: State actors (Russia, China, North Korea) are focusing on quiet, long-term infiltration of critical infrastructure (ICS/SCADA, energy, maritime) for future leverage rather than immediate destruction.

To report several ***Key Cybersecurity Evolutions Driving from Wars:***

- *AI-Driven Weaponization*: AI is transforming cyber-attacks into autonomous operations. Threat actors are using agentic AI for reconnaissance, adaptive malware that rewrites itself, and highly credible deepfakes, according to *CyberWire.*
- *Satellite/Space Frontier*: GPS spoofing and jamming are now routine in 2026 conflict, affecting aviation, maritime8 navigation, and military munitions, as highlighted by *Euronews.com.*
- *Blurring of Crime and War*: State actors are utilizing "proxy" criminal groups for operations, providing plausible deniability while exploiting ransomware for strategic rather than merely financial motives, according to *SecurityWeek.*
- *Digital Sovereignty*: As highlighted in the *WEF Global Cybersecurity Outlook 2026,* nations are reducing reliance on foreign tech (e.g., European firms moving away from specific US cloud providers) to ensure compliance and data protection, leading to regionalized security architectures.

Some ***Key Targets in 2026****:*

- *Maritime Logistics*: Ports and shipping networks are prime targets for operational disruption, notes *Infosecurity Magazine.*
- *Semiconductor Industry*: Continued focus of state-sponsored espionage and disruption, particularly in relation to Taiwan-related tensions, per *Euronews.com.*
- *Healthcare & Energy*: High-value targets for both ransomware and state-backed disruption, according to *ECCU.edu.*

4. *Cybersecurity* was one of the main topics addressed at two of the main international meetings of the beginning of 2026, namely the *Davos World Economic Forum (WEF)* and the *Munich Security Conference (MSC).* We will briefly analyze some of the conclusions of these important meetings regarding the cybersecurity field.

Based on the *World Economic Forum (WEF) Global Cybersecurity Outlook 2026* and discussions from the *2026 Munich Security Conference (MSC)*, the ***cybersecurity***

landscape in **2026** is defined by the acceleration of threats surpassing human defensive capabilities, driven by AI, geopolitical fragmentation, and industrialised cybercrime.

Here are the **Key Cybersecurity Trends for 2026:**

(I) Artificial Intelligence (AI): Supercharging the Arms Race

- AI is the defining factor, with 94% of leaders identifying it as the biggest driver of change.
- *Agentic AI & Automation***:** Attackers are deploying autonomous AI agents that scan networks, discover vulnerabilities, and create exploits in real-time without human supervision.
- *Shift in AI Risk***:** Concerns have pivoted from purely offensive AI to data leaks linked to generative AI (34%) and the advancement of adversarial capabilities (29%), marking a turning point in how organizations manage AI securely.
- *Deepfakes & Synthetic Identity***:** AI-generated audio and video are now mainstream tools for business email compromise (BEC) and financial transaction fraud.

(II) Geopolitical Fragmentation and Cyber Warfare

Geopolitics is a permanent, defining feature of cyber strategy.

- *Hybrid Warfare***:** Cyber operations are increasingly intertwined with military strategy and economic coercion, with 64% of organizations adjusting their strategies to account for geopolitically motivated attacks.
- *Declining Confidence in National Response:* Only 31% of respondents have high confidence in their nation's ability to respond to major cyber incidents, a drop from previous years.
- *Digital Sovereignty***:** Nations are pushing for data localization and sovereign cloud solutions to reduce dependence on foreign technology providers.

(III) ***Cyber-Enabled Fraud and Ransomware Evolution***

- *Fraud Overpowers Ransomware***:** Cyber-enabled fraud (phishing, vishing, smishing) has overtaken ransomware as the top concern for CEOs.
- *Industrialised Crime (CaaS):* Ransomware-as-a-Service (RaaS) has matured, offering "Amazon-like" marketplaces for hackers.
- *Triple Extortion:* Attackers now encrypt data, steal it for leakage, and threaten to attack customers, maximizing payout leverage.

(IV) ***Supply Chain and Critical Infrastructure Vulnerabilities***

- *Third-Party Risk***:** 65% of large companies cite supply chain vulnerabilities as their greatest challenge.
- *OT Security Gaps***:** Operational Technology (OT) remains poorly secured, with only 16% of organizations reporting OT issues to the board.
- *Systemic Concentration Risk***:** The reliance on a few major cloud and internet service providers creates a "single point of failure" scenario for the global economy.

(V) *The Resilience and Capability Gap*

- *Resilience Gap Widening*: The disparity between large, highly resilient organizations and smaller, under-resourced firms is growing.
- *Skills Shortage*: 85% of organizations with low resilience lack critical cybersecurity skills.
- *Zero Trust as Standard*: By 2026, 81% of organizations plan to adopt Zero Trust architecture due to the failure of traditional VPN-based perimeter security.
- *Post-Quantum Preparation*: "Harvest now, decrypt later" attacks are forcing early adoption of post-quantum cryptography.

Key Takeaways for 2026 Strategy:

- *Move from Prevention to Resilience*: Assume breach and focus on rapid recovery.
- *Govern AI Adoption*: 64% of organizations are now assessing the security of their AI tools, up from 37% in 2025.
- *Collaboration:* Collective cyber resilience is a strategic mandate; sharing threat intelligence with peers and government is essential.

To conclude, the primary cybersecurity trends emerging in 2026 center on *agentic and offensive AI weaponization, geopolitical fragmentation*, and *elevated nation-state threats to critical infrastructure*.

Data and consensus from the *World Economic Forum (WEF) Davos 2026 Annual Meeting, the Munich Security Conference (MSC) 2026*, and the *G7 Summit* in Évian establish that *cyber risk is no longer just an IT concern, but a core element of economic strategy and national security*.

The acceleration of ***artificial intelligence*** has supercharged both cyberattack capabilities and defensive strategies, causing global leaders to identify AI-driven fraud and vulnerability as top security threats.

To combat this, global forums emphasize moving from basic compliance to measurable ***cyber resilience*** and implementing systemic, cross-border threat intelligence.

Furthermore, the convergence of geopolitics and digital operations has made securing ***critical infrastructure*** against state-sponsored disruptions and disinformation a vital component of national security. Consequently, leaders at these summits continue to strongly advocate for collaborative ***public-private partnerships*** to ensure digital sovereignty and safely govern emerging technologies.