"Cyber intelligence and international security in 2026"

Managing cybercrime to break the regulatory and diplomatic silence on the digital operations of states. A strategic analysis of the cyber operations of states, the grey area of international law and the implications for global security considering the US-Iran conflict.

by
Federica Maria Rita Livelli and Antonio Albanese

“Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters, and constellations of data. Like city lights, receding...”

William Gibson, Neuromancer

Table of Contents

Executive Summary

The context of geopolitical and geoeconomic permacrisis and polycrisis in 2026 requires the ability to analyse the cyber intelligence and international security landscape, with particular attention to the management of cybercrime in the digital operations of states.

Moreover, as Europe grapples with new geopolitical realities, the need for a comprehensive approach to security has never been more pressing. The changing dynamics of global alliances and the increasing complexity of cyber threats, especially with the integration of artificial intelligence into hybrid warfare, highlight a fundamental truth: modern warfare is not based on military power alone.

Therefore, the goal is to contribute to overcoming the legal and diplomatic silence that surrounds state cyber operations, opening a structured debate on norms, responsibilities, and international cooperation.

It should be noted that 2026 marked an epochal turning point: the armed conflict between the US-Israel and Iran (Operation Epic Fury / Operation Roaring Lion, February 28, 2026) has definitively consecrated cyberspace as the integral operational domain of modern conflicts. Cyber operations have preceded, accompanied, and amplified kinetic attacks, demonstrating the inseparability between digital and conventional warfare.

In fact, as also reported by the Clusit Report – March 2026, the year just ended, was an *annus horribilis* with a further increase in cyber-attacks in the face of the ongoing geopolitical crises.

1. The US-Iran conflict 2026: cyber as the fifth operational domain

The intent of the white paper is to provide the chronology of what has happened from the beginning of the conflict to better understand the dynamics of cyber intelligence and field of action.

1.1 Anatomy of a hybrid conflict

On February 28, 2026, the United States and Israel launched joint military operations against Iran - i.e. *Operation Epic Fury (USA)* and *Operation Roaring Lion (Israel)* - marking the culmination of a multi-year escalation. For the first time in the history of modern conflicts, cyber operations deliberately preceded kinetic strikes with the explicit aim of leaving the enemy "*disrupted, disoriented and confused*", in the words of General Dan Caine, Joint Chiefs of Staff of the US Armed Forces.

Cyber operations were divided into three simultaneous levels:

1. disruption of Iranian command, control, and communication systems;
1. information operations to fuel internal dissent and destabilize the regime;
2. degradation of critical digital infrastructures.

In addition, Iranian internet connectivity plummeted to 1-4% of normal levels for over 60 hours, in what some Israeli sources called "the largest cyberattack in history."

Timeline of cyber operations in the US-Iran conflict (February - April 2026)

February 28, 2026	**US-Israel coordinates:** *pre-kinetic cyber strike* on Iranian C2 networks; BaadeSaba app (prayer) compromised for disinformation; *takedowns* of state media channels.
February 28–March 1, 2026	**Internet blackout:** Iran connectivity at 1-4%; over 60 hours of total disruption.
1- 2 March 2026	**Hacktivist counterattack:** >60 pro-Iran groups activated; Russian NoName057(16) group joins operations; DDoS attacks on Israeli payment systems and Kuwaiti government sites.
March 11, 2026	**Stryker Attack:** Handala Hack (MOIS) Targets US Medical Company with Destructive Malware; 50TB of Exfiltrated Data; 17 Days of Operational Recovery.
March 19, 2026	**DOJ response:** U.S. Department of Justice dismantles 4 pillars of MOIS-Handala infrastructure; $10 million offer for information on Iranian cyber actors.
April 17, 2026	**Partial Internet Restoration:** Iran begins to restore limited internet, only on the National Information Network.

1.2 The grey area of legitimacy: cyber-attacks as acts of war?

The 2026 U.S.-Iran conflict has raised many questions about the applicability of international law to cyberspace. In fact, the cyber operations that preceded and accompanied the kinetic operations operated in a regulatory vacuum: neither the law of armed conflict nor the UN Charter offer a definitive answer as to when a cyber operation constitutes "use of force".

The compromise of the BaadeSaba app — one of the most popular prayer apps in Iran — to send subversive messages to millions of users is a prime example of an operation on the border between espionage, *information warfare,* and psychological operation. Classical international law does not provide tools to categorize, and therefore regulate, this type of action.

In addition, the 47-day interruption of internet connectivity — attributed to a combination of physical strikes on data centres and cyber disruption — constitutes a potential attack on civilian infrastructure, prohibited by international humanitarian law.

However, the impossibility of distinguishing between military and civilian infrastructures in cyberspace makes the application of these rules extremely complex.

US-Israeli operations	Answer Iran / Pro-Iran
Pre-positioning cyber pre-kinetic	Global hacktivist network activation
Destruction of Iranian C2	Destructive malware on US targets (Stryker)
Civilian app compromise (BaadeSaba)	DDoS regional financial infrastructure
State media takeover (IRNA - Islamic	Data exfiltration and transaction leaks

Republic News Agency)	
Access security cameras - Tehran	Targeting OT/ICS (Rockwell Automation)
Campagne IA anti-regime su social media	Campagne phishing anti-israeliane (APK APK malevolo RedAlert)

1.3 Strategic implications: new paradigms of deterrence

The 2026 U.S.-Iran conflict highlighted how Iran — which "lacks symmetrical conventional response options" (CSIS - Center for Strategic and International Studies, 2026) — has made massive use of cyberspace and proxy networks as a tool of asymmetric deterrence and retaliation. This dynamic is not new, but it will reach unprecedented scale and sophistication in 2026.

The use of hacktivist proxies — from Handala Hack (MOIS) to globally distributed autonomous groups — introduces structural complexity in cyber deterrence: when cyber operations "go beyond the scope of military operations themselves" (CSIS, 2026), the classic mechanisms of escalation and de-escalation lose effectiveness. "Plausible deniability", historically a strategic advantage, becomes a factor of systemic instability.

A further element of complexity is represented by the convergence between state and criminal groups: the *CL-STA-1128 (Cyber Av3ngers)* group, identified by Palo Alto Networks Unit 42 in March 2026, demonstrated OT (Operational Technology) / ICS (Industrial Control Systems) capabilities on Rockwell Automation systems, signalling an increase in the quality of Iranian threats to Western industrial infrastructures.

2. The international regulatory vacuum: legal and diplomatic silence

As far as the current legal architecture is concerned, it is necessary to highlight its limitations.

In fact, existing international law was not designed for cyberspace. Three sets of regulations are partially applicable - i.e. the Law of Armed Conflict (IHL), the Law of Peaceful International Relations (UN Charter) and International Criminal Law – but none adequately covers cyber state operations in their specificity.

The *Tallinn Manual* (2.0, 2017) represents the most systematic academic attempt to apply existing international law to cyberspace, but it remains a non-binding document, drawn up by independent experts, with little transposition into the practice of states.

Moreover, the differences in interpretation between the great powers — the United States, Russia, China — make it impossible to reach a consensus on minimum standards of behavior.

Hereafter a table containing the main gaps in international law in cyberspace.

The four main gaps in international law in cyberspace	
1	**Attribution:** absence of binding international mechanisms for the attribution of cyber operations to the responsible states; structural "plausible deniability" makes liability elusive
2	**Threshold of the use of force:** lack of a shared definition of when a cyber operation constitutes "use of force" (Art. 2(4) UN Charter) or "armed attack" (Art. 51), which justifies legitimate defense

3	**Civilian infrastructure protection:** IHL's distinctions between military and civilian objectives are difficult to apply to dual infrastructures (internet, energy systems, financial networks)
4	**Cyber espionage:** International law does not traditionally regulate espionage — not even cyber espionage — creating a grey area in which SIGINT and offensive operations overlap

2.2 The diplomacy of silence: why states do not speak

It should be noted that the "diplomatic silence" on state cyber operations is not accidental, but structural. States avoid codifying binding norms in cyberspace for converging strategic reasons, regardless of geopolitical location.

The great powers - i.e. the USA, Russia, China and Israel - have invested massively in cyber offensive capabilities and do not intend to limit them through international agreements. On the other hand, developing countries fear that international norms will be used by established powers to maintain digital hegemony; while other players - such as Iran, North Korea, non-state groups - use the regulatory vacuum as an asymmetrical competitive advantage.

The US-Iran 2026 conflict has further shown how dangerous this silence is: without shared norms, *miscommunication* and *misperception* can transform cyber intelligence operations into acts interpreted as *casus belli*.

In addition, the "contamination" of tools — from *wipers* to *ransomware*, from *DDoS* to the manipulation of civilian apps — makes it increasingly difficult to distinguish between *crime, warfare* and espionage.

2.3 Attempts at governance: Budapest, GGE and their limits

The *Budapest Convention on Cybercrime* (*Budapest Convention on Cybercrime* 2001) remains the main international instrument of cooperation against cybercrime, with 68 States Parties.

However, Russia and China have not ratified it, and its scope explicitly excludes state operations. The subsequent *Additional Protocol* (*Additional Protocol to the Convention on Cybercrime* - 2022), while improving procedural cooperation, does not address state operations.

In addition, the *United Nations Groups of Governmental Experts (GGE)* (2010-2021) have produced consensus reports that recognize the applicability of international law to cyberspace and identify eleven non-binding norms of responsible behavior.

It is necessary to inform that, despite the *OEWG (Open-Ended Working Group) process* continuing, the divisions between Western blocs and Russia-China remain, limiting progress, preventing the establishment, to date, of a verification or enforcement mechanism.

3. Attribution models and intelligence sharing: best practices

Below is an overview of the various attribution models and intelligence sharing, along with their best practices.

3.1 Attribution as a diplomatic tool

The public attribution of cyber operations has become a fundamental political-diplomatic tool to "break the silence", transforming operations in the grey area into events with names, responsibilities and consequences. The *NotPetya* case (2017) set the precedent, namely: a joint

statement, coordinated by the United States, the United Kingdom, New Zealand, Australia and Canada, publicly attributed the attack to Russia, constituting the first systematic form of deterrence by regulation.

The following is an example of a multi-level attribution framework referring to the NotPetya-SolarWinds model

Multi-Level Attribution Framework: The NotPetya-SolarWinds Model	
STEP 1	**Technical correlation:** malware forensics, TTPs (Tactics, Techniques, Procedures), C2 infrastructures; use of MITRE ATT&CK framework for threat actor fingerprinting
STEP 2	**Geopolitical analysis:** contextualization of objectives in the framework of international relations; historical patterns of behavior of the alleged state actor
STEP 3	**HUMINT validation:** confirmation of state origin through human sources; crucial for distinguishing between direct operation, proxy and false flag
STEP 4	**Intelligence sharing:** multi-lateral sharing with allies through classified channels (Five Eyes, EU INTCEN, NATO CCDCOE) to build pre-announcement consensus
STEP 5	**Coordinated public statement:** simultaneous announcement from multiple capitals to maximize diplomatic impact and minimize denial capabilities

3.2 The EU INTCEN framework and structured sharing

The *EU INTCEN* (*European Union Intelligence and Situation Centre*) programme represents the most advanced model of *cyber intelligence sharing* between democracies. Through standardized platforms - such as MISP (*Malware Information Sharing Platform*) and *STIX (Structured Threat Information eXpression) / TAXII* (*Trusted Automated eXchange of Intelligence Information*) protocols - Member States share IoCs (*Indicators of Compromise*) preserving the protection of HUMINT sources through strategic anonymization processes.

The model is divided into gradual classification levels, allowing the progressive declassification of information to maximize collective protection, without compromising sensitive sources. In addition, the feedback loop between receiving agencies and senders ensures the continuous contextual enrichment of shared intelligence.

The U.S.-Iran conflict has highlighted, in fact, the need to extend this model as the speed with which the 60+ hacktivist groups have been activated — many operating from outside Iran, through Starlink and other VSAT services — has required real-time intelligence coordination that existing mechanisms struggle to sustain.

3.3 The Estonian model: legal framework for the state response

The massive DDoS attacks against Estonia in 2007 - i.e. the first documented case of cyber aggression against a sovereign state - produced the most advanced response in terms of legal-operational framework.
Estonia has developed a model that integrates:

- military dimension (*Cyber Defense Unit* with a clear mandate on intervention thresholds)
- civil dimension (formalized public-private partnership)
- international dimension (*NATO Cooperative Cyber Defence Centre of Excellence -CCDCOE)* as a hub for the standardization of response doctrines.

The key element of the Estonian model is the clear legal definition of when a cyber action exceeds the threshold of "use of force" according to Article 2(4) of the UN Charter. Such domestic regulatory clarity — even in the absence of an international consensus — allows Estonia to respond in a proportionate and legally based manner to operations that other states would be forced to ignore or "scale" in an uncalibrated way.

3.4 Intelligence-led policing: the Emotet case and civil-military convergence

The Europol Joint Operation to dismantle the *Emotet botnet* (2021) remains the most significant case study of convergence between cyber intelligence, law enforcement, and international cooperation.

In fact, the synchronization of 8 jurisdictions for the simultaneous execution of the *takedown* - with neutralization of the infrastructure and replacement of the payload - demonstrated the operational feasibility of *cross-border cooperation*.

That is, the operation – at the level of lessons learned – has shown how even against apparently non-state cybercrime, the multi-disciplinary *intelligence-driven* approach is essential, since criminal groups can be proxies of states.

In addition, the line between *organized cybercrime* and *state-sponsored operations* is structurally porous - as confirmed by the relationships between Hydra (Russia - Hydra Market was the largest and longest-running Russian-language marketplace on the dark web until its closure in April 2022), Lazarus Group (North Korea.

The Lazarus Group is a North Korean state-sponsored hacker collective, also known as APT38, that conducts cyberespionage activities globally and financial theft to fund the regime. Operating since at least 2009, it is known for the 2014 Sony Pictures cyberattack, the 2016 Bank of Bangladesh robbery - $81 million - and the 2017 WannaCry ransomware attack), and, in 2026, by Handala Hack (Iran - The group serves as a cover for Void Manticore - also known as Storm-0842 or Banished Kitten, a unit affiliated with the Iranian Ministry of Intelligence and Security. MOIS. It is the group that recently penetrated FBI Director Kash Patel's account and emails in March 2026).

4. The threat landscape in 2026: geopolitical cases and scenarios

Hereafter an overview of the threats and the main cases of cybercrime in recent years and lessons learned and best practices.

4.1 Main State Cyber Crime Cases (2024-2026)

Russian Cyber Campaign against Ukraine (2024): +70% - Russian cyberattacks against Ukraine increased by almost 70% in 2024, with 4,315 documented incidents targeting critical infrastructure, government services, the energy sector, and defense-related entities.
The campaign demonstrates the systemic integration between cyber warfare and conventional kinetic conflict, with cyber operations used to degrade defensive and communication capabilities before physical attacks.

Chinese cyber espionage (2024): +150% and +300% in Manufacturing - Chinese cyber espionage operations have experienced unprecedented growth in 2024. The semiconductor sector is identified as particularly vulnerable, in relation to competition with TSMC and US export restrictions.

Google identifies China as the most sophisticated and widespread industrial espionage threat in the world, with a focus on intellectual property in strategic sectors: AI, quantum computing, advanced military technologies.

Attack on the U.S. Treasury Department (December 2024) - Chinese hackers have hacked a third-party vendor of the U.S. Treasury Department, gaining access to over 3,000 unclassified files. The case emphasizes the issue of supply chain vulnerabilities: the attacker did not attack the US government head-on but exploited a weak link in the supply chain. Response best practice requires multi-layered supplier validation, Zero Trust architectures to limit lateral movement, and XTI platforms for continuous supply chain monitoring.

ByBit Theft: $1.5 Billion in Ethereum (February 2025) - North Korean hackers stole $1.5 billion worth of Ethereum from Dubai-based exchange ByBit, setting the world record for cryptocurrency theft attributed to a nation-state.
The case illustrates Pyongyang's strategy of using financial cybercrime as a source of revenue for its nuclear program, i.e., a unique model on the international scene that dissolves the distinction between crime and state policy.

4.2 Geopolitical scenarios 2026: the new international cyber order

Below are the various geopolitical scenarios that are characterizing 2026.

Russia-NATO Hybrid Warfare - Digital Escalation
The Russian-Ukrainian conflict continues to be the most advanced laboratory of hybrid warfare. While not directly involved, NATO has begun to respond to Russian "grey zone" operations with more aggressive *cyber offensive* actions, marking a significant doctrinal shift.
Moreover, the escalation of attacks on European energy infrastructure, transport systems and communication networks, combined with disinformation operations against electoral processes, configures a level of aggression that challenges the traditional categories of international law.

US-China Competition - The Chip War
The US-China technological competition manifests itself with increasing intensity in cyberspace. Industrial espionage against semiconductor manufacturers – i.e. TSMC, Intel, Samsung – is systematic and documented. In addition, the export restrictions on EUV and AI technologies imposed by Washington accelerate Beijing's cyber response, which seeks to acquire - through clandestine operations - what it cannot obtain commercially, as well as develop its own AI chips.

Iran - Cyber as asymmetrical deterrence - The ongoing conflict has revealed the full maturity of Iran's cyber capabilities. That is, Iran has shown that it knows how to combine direct state operations with globally distributed *hacktivist proxy* networks, operating autonomously even during the domestic internet blackout through VSAT and Starlink services.
In addition, the targeting of OT/ICS systems (Rockwell Automation, energy SCADA systems) highlights a qualitative evolution towards destructive capabilities on Western critical infrastructures.

North Korea - The State Cyber Crime Model
The Lazarus group and its affiliated operations continue to represent the most extreme case of "fusion" between the State and cybercrime. With the ByBit theft, Pyongyang has demonstrated the ability to carry out offensive financial operations worth billions of dollars, directly financing the weapons program.
In addition, the infiltration of global tech companies through operations under false identities — identified by Microsoft in 2025 — introduces a supply chain risk vector that is difficult to counter.

5. Operational framework: validation cycle and integrated cyber intelligence

It follows a roadmap for implementing the integrated cyber intelligence operational framework.

5.1 The intelligence cycle: from OSINT to political decision making

Effective management of state-based cyber threats requires an operational framework that integrates OSINT, HUMINT and technical analysis into a structured cycle of collection, validation, and dissemination.

It should be noted that the SolarWinds case (2020) remains a fundamental methodological reference, considering that the human element was instrumental in identifying the campaign as Russian state espionage — and not ordinary cybercrime — and in assessing the strategic scope beyond the technical data.

Below is an outline of the 6-step cyber intelligence cycle

THE CYBER INTELLIGENCE CYCLE	
STEP 1	**AUTOMATED COLLECTION** - OSINT, Network Monitoring, Honeypots, Dark Web Feed, Commercial Threat Intelligence
STEP 2	**AI/ML TECHNICAL ANALYSIS** - Pattern recognition, anomaly detection, IoC correlation, clustering TTPs (Tactics, Techniques, and Procedures).
STEP 3	**CRITICAL HUMAN VALIDATION** - Senior analysts verify false positives, contextualize geopolitically, evaluate the actor's motivations.
STEP 4	**HUMINT ENRICHMENT** - Confirmation and in-depth analysis through human sources; cross-source verification; reliability evaluation.
STEP 5	**SUMMARY AND ATTRIBUTION** - Actionable intelligence document; level of confidence on attribution; response options.
STEP 6	**POLITICAL DECISION** - Diplomatic, legal, technical, or military response; Allied coordination; public communication

NOTE
Phase 3 - Critical Human Validation is the focal point of the entire cycle, considering that no AI/ML system, no matter how advanced, can replace the contextual judgment of a senior analyst in distinguishing between a state-sponsored attack and an opportunistic cybercriminal operation, or in assessing the geopolitical implications of a public attribution.

In the context of the US-Iran 2026 conflict, the speed with which proxy operations activated by geopolitically heterogeneous actors (pro-Iran, pro-Russia, autonomous hacktivists) overlapped, made human validation even more critical and increasingly a strategic asset.

5.2 Best practices for 2026: Operational priorities

Below are some of the best practices and priorities to consider in the face of the contingent geopolitical scenario.

Zero Trust Architecture – Implementing Zero Trust — "*never trust, always verify*" — has become the top priority for organizations and government agencies. According to various reports from the cybersecurity industry, 96% of global organizations favour this approach, while 81% are in the process of being implemented. Fundamental principles include continuous identity verification, least privilege (JIT access), network micro-segmentation, and *continuous monitoring* of all sessions and connections.

AI-automated SOCs - In 2026, AI will move from experimental deployments to fully integrated components in *Security Operations Centers (SOCs).* AI is no longer limited to anomaly detection but spans the entire incident cycle - automated *threat identification, prioritization, containment,* and *remediation*.
In addition, AI-powered SOAR (*Security Orchestration, Automation and Response*) systems free up human analysts for more complex geopolitical context analyses, i.e. the area where the human factor remains irreplaceable.

Post-Quantum Cryptography (PQC) - Quantum computing reaches a tipping point in 2026 that requires urgent migration to *Post-Quantum Cryptography (PQC).* Therefore, organizations are advised to: inventory all systems that use vulnerable asymmetric cryptography; implement "*crypto-agility*" to allow the rapid switching of algorithms; participate in NIST standardization programs.
In fact, it should be noted that state actors – in particular, Russia and China – are accumulating encrypted data today in anticipation of decrypting it when quantum computing is mature (i.e. "*harvest now, decrypt later*" strategy).

Resilience as a core strategy - The paradigm is shifting from total prevention - now recognized as impossible - to resilience as a fundamental operational strategy. It follows that organizations must assume that compromise is inevitable and plan according to this assumption, by defining: *Business Continuity Planning* with specific cyber-attack scenarios, *realistic Recovery Time Objectives (RTOs),* and *Recovery Point Objectives (RPOs); quarterly tabletop exercises* with current geopolitical scenarios.

6. Policy recommendations: breaking the legal and diplomatic silence

Below are some strategic recommendations to break the legal and diplomatic silence.

6.1 International community and governments

It should be noted that overcoming diplomatic silence on state cyber operations requires a multi-layered approach, combining binding legal obligations, new institutional mechanisms, and structured diplomatic incentives. The following recommendations arise from the analysis of the case studies and dynamics of the US-Iran conflict 2026.

Priority recommendations for governments and international organizations	
International Cyber Tribunal	Establishment of a specific jurisdiction for state cybercrime, with competence over the certified attribution of operations, like the International Criminal Court but with mechanisms adapted to the specificity of the digital domain
Extension of the Geneva Conventions to cyberspace	Additional Protocol defining cyber weapons, identifying protected civilian infrastructure (hospitals, water systems, power grids), and establishing proportional intervention thresholds
Mandatory transparency reporting	Obligation for states to declare their offensive cyber capabilities — modelled on arms control treaties — as a prerequisite for building international trust
Coordinated multi-lateral sanctions	Automatic multilateral sanctions mechanisms for violations ascertained by certified international bodies, reducing dependence on contingent political consensus
Cross-country cyber hotline	Direct communication channels for the de-escalation of cyber crises, analogous to the nuclear hotlines of the Cold War, with notification protocols for operations with a high risk of misperception
European Union Vulnerability Database	Further promote the European Catalogue of Actively Exploited Vulnerabilities, harmonized with the U.S. CISA KEV, for evidence-based prioritization of patches and a coordinated response

Critical Infrastructure Organizations - Organizations operating in critical industries — i.e., energy, finance, healthcare, defense, space, etc. — face threats that combine government capabilities with criminal objectives. Therefore, they should consider the following integrated recommendations that consider the geopolitical landscape of 2026.

Energy and Critical Infrastructure Sector	Financial Sector
Rigorous OT/IT segmentation with physical air gaps	**Preparing for** attacks on SWIFT systems and payments
Threat intelligence feed specifici per APT energy-targeting	**Crypto-asset security** contro *state-sponsored heist*
Black-start drills (full reboot)	**Sanctions compliance automation** contro *money laundering*
Collaboration with CISA/ENISA for early warning	**Partnering with FinCEN** for anomalous flow intelligence
Protection of SCADA systems from Iranian and Russian actors	**Incident response plan** for digital asset theft

Healthcare e Pharma	Aerospace & Defense
Vaccine and Therapeutic Research Data Protection	**Continuous threat hunting** vs. *Assume persistent breach:*
Resilience planning con *patient safety* come priorità	***ITAR (International Traffic in Arms Regulations) /EAR (Export Administration Regulations)*** compliance automation
Segmentation of *medical devices* from general IT networks	**Collaboration** with *defense intelligence* for attribution
Intelligence on targeting from hostile states (biotech)	**Quantum-safe encryption (QSE)** for classified communications
Backup immutabili e Recovery Point Objective < 4h	**Supply chain verification** for critical components

6.3 The role of the human factor in cyber intelligence

The advancement of AI technologies risks obscuring a fundamental truth, namely: the human factor remains the central and irreplaceable element of cyber intelligence. These are not only analysts who validate technical data, but professionals capable of reading the geopolitical context, understanding the motivations of the actors, and translating technical intelligence into subsequent calibrated political decisions made by the authorities in charge.

Psychological manipulation — i.e. social engineering, deepfakes, AI-created disinformation campaigns — demonstrates how humans remain the most vulnerable critical infrastructure. In the 2026 U.S.-Iran conflict, the BaadeSaba app compromise and AI-enabled disinformation campaigns against the Iranian regime have, in fact, operated on the psychological and cognitive, not technical, dimension of the conflict.

Therefore, the convergence of *Cyber Intelligence*, *OSINT* and *HUMINT* requires a radically integrated approach, considering that automation manages volume and speed, while the human element ensures quality, context, and accountability. Only through this balance is it possible to avoid errors of assessment with significant geopolitical consequences, such as the misidentification of an espionage operation as an act of war, or vice versa.

7. Conclusions: towards an international cyber governance regime

2026 represents an epochal turning point for international cyber security. The US-Iran conflict has further demonstrated that cyberspace is the fifth domain of war, inseparable from land, sea, air, and space. In fact, the convergence between cybercrime, cyber warfare, and cyber intelligence - already theorized - is increasingly a documented operational reality.
It follows that legal and diplomatic silence on states' cyber operations is no longer sustainable. Not because it is required by abstract ethical considerations, but because it has become a source of systemic instability: the lack of shared norms increases the risk of misperception, unintentional escalation, and uncontrolled proliferation of offensive capabilities.

In fact, if the Stuxnet case of 2010 opened a real Pandora's box, the US-Iran 2026 conflict has definitively highlighted the need for cyber governance.

It is necessary to point out that, although the road to an international regime of cyber governance is long and difficult, it is not impossible, especially remembering how the Cold War arms control treaty model - patiently built between deep ideological adversaries - offers a lesson in method: cooperation on minimum standards of behavior does not require mutual trust, but only the shared recognition that total instability is worse than the negotiated limitations.

Moreover, in this content of perma-crisis and poly-crisis, organizations must increasingly ensure resilience and invest in the human element of cyber intelligence, as well as actively participate in the construction of an ecosystem of international cooperation.
Cyberspace cannot remain the "Wild West" of international security: the stakes – i.e. critical infrastructure, financial systems, and human lives – are too high.

Therefore, to overcome legal and diplomatic silence, it will be a matter of:

- **Start negotiations for a further additional protocol** to the Geneva Conventions on cyberspace, with a binding definition of *cyber weapons* and protections for civilian infrastructure
- **Establish a Group of International Experts** for the certification of cyber attribution, to support the coordinated public statements of Allied States
- **Build a system of bilateral cyber hotlines** between the major powers (US-Russia, USA-China, NATO-Russia) for the de-escalation of digital crises
- **Adopt minimum international standards of transparency reporting** on offensive cyber capabilities, including the issue in the G7 and G20 agenda
- **Accelerate global migration to post-quantum cryptography** before quantum computing deprecates current classified communications security systems
- **Investing massively in the training of cyber intelligence analysts** with integrated skills: technical, geopolitical, and international legal

In conclusion, the speed with which cyber events propagate requires intelligence systems capable of anticipating, interpreting, and responding to borderless threats and unprecedented forms of digital conflict.

Datum, in Latin, meant "that which is given" — a point of departure, not a point of arrival. Today, data is the fundamental element from which every cognitive process starts, i.e. they must be collected, shared, processed to generate information useful for action.

Moreover, validation through multiple sources is not a methodological option, but a condition for operational survival. Equally crucial is the timely integration of this information into decision-making processes - from crisis management to the protection of critical ecosystems - without forgetting that no technology can replace the political responsibility to break the silence and build a shared cyber governance, based on digital diplomacy that finally lives up to the stakes.

The fight against new forms of conflict therefore requires a profound metamorphosis: a shared legal framework and cyber diplomacy not only as a tactical tool for collecting information but also as an information intelligence architecture.

Sources and References

This White Paper is based on primary open-source research sources, government documents, and private intelligence reports updated as of April 2026. Below are the main reference sources.

Institutional primary sources:

- CISA (Cybersecurity and Infrastructure Security Agency) - Nation-State Cyber Actors (cisa.gov)
- Center for Strategic and International Studies — Significant Cyber Incidents Database 2024-2026 (csis.org)
- Canadian Centre for Cyber Security — Cyber Threat Bulletin: Iranian Cyber Threat Response, (Febbraio 2026)
- Palo Alto Networks Unit 42 — Threat Brief: Escalation of Cyber Risk Related to Iran (aggiornato ad Aprile 2026)
- U.S. Department of Justice — Justice Department Disrupts Iranian Cyber-Enabled Psychological Operations (Marzo 2026)
- CSIS — How Will Cyber Warfare Shape the U.S.-Israel Conflict with Iran? (Marzo 2026)

Threat intelligence reports:

- Microsoft Security Intelligence — 2025 Review: Nation-State Cyber Operations
- Google Threat Intelligence Group / Mandiant — Annual M-Trends Report 2025
- Flare.io — Monitoring Cyberattacks Directly Linked to the US-Israel-Iran Military Conflict
- SentinelOne — Cybersecurity Trends and Nation-State Actors 2025-2026
- Accenture — State of Cybersecurity 2025
- CrowdStrike — Global Threat Report 2025

Framework and technical documentation:

- MITRE ATT&CK Framework — Enterprise Matrix v15
- NIST — Post-Quantum Cryptography Standards (FIPS 203, 204, 205)
- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017)
- EU NIS2 Directive — Directive (EU) 2022/2555
- World Economic Forum — Global Cybersecurity Outlook 2026

Italian and European sources:

- CybersecItalia — Cyberspace: the EU agenda to prevent terrorism
- CybersecItalia — Beyond the technological perimeter: human factor, psychological manipulation, and human-centric defense
- AgendaDigitale — Geopolitics of AI: the new global power play in a world without arbitrators
- ISMS.online — The line between nation-states and cybercrime is blurring: that's bad news for CISOs
- Bytelegali — Pierguido Iezzi: the real critical infrastructure today is the human being