Observatoire ARGA

Report on Sanctions and Compliance for 2025

DIGITAL SURVEILLANCE TECHNOLOGIES IN AUTHORITARIAN REGIMES

Spyware Infrastructure, Commercial Interception Systems, Transnational Operations, and Threats to International Security

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA – Sanctions and Compliance Division

Correspondence Address: 14 rue Jacques Laffitte, Bayonne, 64100

Contact: info@argaobservatory.org

Paris, 18 November 2025

Table of Contents

Executive Summary

Digital surveillance technologies provide authoritarian states with tools of control comparable in power to traditional intelligence agencies, but operating faster, more covertly, and transnationally. Over the past decade, a new infrastructure of political-digital oversight has emerged across Eurasia— a hybrid of commercial spyware solutions, state data-processing centers, social-media monitoring systems, network-injection devices, and cross-border mechanisms of unauthorized access to personal devices.

This is not a collection of disparate instruments, but a coherent system capable of tracking movements, communications, financial transactions, personal networks, and behavioral patterns of specific groups and elites. The new surveillance architecture integrates traffic-interception technologies, mobile OS exploits, IMSI-catchers, behavioral analytics, facial recognition, messenger-level surveillance tools, penetration into Telegram clusters, cryptocurrency-wallet interception, and telecom-infrastructure data harvesting.

Digital surveillance has become not only a mechanism of internal control — authoritarian regimes now use it as an instrument of external operations. Persecution of opposition figures, businesspeople, refugees, and whistleblowers occurs beyond national borders: spyware is deployed in the EU, the US, Turkey, and the UAE; diplomatic missions serve as distribution hubs for malicious software; "remote hacking units" of mobile devices operate from within foreign jurisdictions.

Digital monitoring becomes the basis of hybrid operations — it is used for fabricated criminal cases, corporate raids, asset seizures, pressure on families, access to private correspondence, financial data, documents, and digital traces. In some cases, technologies of "digital torture" have been documented — attempts to break a person psychologically through threats, mass notifications, leaks of private information, or deepfake kompromat.

The ARGA Observatory examines this system as a phenomenon of next-generation digital authoritarianism — a supranational and technocratic structure that turns surveillance into a universal political instrument operating outside legal frameworks and beyond national boundaries.

1. Methodology

This report is based on a multi-layered study of digital surveillance infrastructures in authoritarian Eurasian states, with emphasis on technical analysis of spyware systems, their suppliers, vectors of deployment, and use against individuals abroad.

The core source base includes OSINT data, technical attribution of network nodes, judiciary and human-rights documentation, as well as field reports collected from experts, lawyers, IT analysts, and victims of digital persecution.

The research relies on:

— OSINT and TECHINT data: domain correlations, SSL certificates, imported lawful-interception equipment, IP logic of C2 servers.

— Analysis of spyware and commercial surveillance infrastructure: Pegasus-like tools, Predator, Candiru, FinFisher, Intellexa, RCS Lab.

— Monitoring cases of digital persecution of activists, politicians, journalists, entrepreneurs, lawyers, and emigrants.

— Court materials from the EU and the US, UN WGAD submissions, and findings of UN Special Rapporteurs.

— Investigations by Citizen Lab, Amnesty Tech, OCCRP, The Markup, Forbidden Stories.

— Interviews and confidential consultations with digital-security experts (anonymized).

— ARGA Observatory's internal research on spyware, digital harassment, and Interpol Abuse (2020–2025).

Analytical approach

All incidents and case studies in the report were verified through a dual-channel method:

1. confirmation through technical artifacts (logs, C2 routes, forensic infection traces), and
2. confirmation through independent sources (media investigations, court documents, expert information).

The geographical scope includes Russia, Belarus, Kazakhstan, Azerbaijan, Uzbekistan, Kyrgyzstan, Armenia, Georgia, as well as external operations of these states in the EU, Turkey, the UAE, and the United States.

Research limitations

Some operations remain undocumented due to the absence of court proceedings, but all included cases are technically and evidentially substantiated. Estimates of the scale of digital surveillance use conservative coefficients, considering the opaque nature of the spyware market.

2. Introduction: Digital Control as the Foundation of Modern Authoritarianism

In the 21st century, digital surveillance has become not an auxiliary element of state security but the foundation of authoritarian governance. Surveillance technologies are no longer limited to selective interception of communications — they are integrated into political management, judicial processes, economic conflicts, and international operations against opponents. Control over communications means control over society, and access to digital traces enables the management of elites, businesses, and population flows.

Authoritarian regimes in Eurasia view digital infrastructure as a tool of strategic power. Surveillance technologies simultaneously perform several functions:

— suppress political activity at an early stage;

— capture communications and networks for future coercive use;

— enable profiling of elites based on risk and loyalty;

— ensure business control through the threat of data exposure;

— serve as a platform for fabricating criminal cases and running information attacks;

— extend the reach of security agencies far beyond national borders.

This surveillance regime targets not only activists and journalists. Entrepreneurs, officials, lawyers, IT specialists, migrants, and political refugees all fall under monitoring. Digital control becomes a method for keeping capital inside the country, a tool of corporate warfare, and a means of pressuring the families of those who have relocated abroad. Spyware, messenger interception, monitoring of banking transactions, and surveillance of cloud services form a unified architecture of influence — from personal devices to international platforms.

The external dimension is no less important than the internal one. Authoritarian states have learned to use digital oversight for cross-border operations: tracking emigration routes, cryptocurrency traffic, communications among opposition groups abroad, attempts at extradition, and disinformation or smear campaigns through media and social networks. Surveillance has become as much a part of foreign policy as diplomacy or security operations.

Thus, digital control is not merely a technological practice but a new political architecture. It replaces institutions of trust, compensates for weak judicial mechanisms, enables the retention of power, and expands authority beyond national boundaries. Spyware, DPI interception, big-data monitoring, and machine profiling turn intelligence services into a hybrid digital apparatus operating in a mode of continuous observation.

3. Architecture of Digital Surveillance

Digital surveillance in the authoritarian regimes of Eurasia is not a collection of separate systems — it is a multilayered infrastructure in which state monitoring centers, commercial spyware solutions, and shadow criminal structures operate as a single mechanism. Control over communications, data, and devices creates a full cycle of coercive influence: information collection → analytical processing → operational application → political and security pressure.

ARGA Observatory identifies four systemic layers of digital surveillance.

3.1. State Monitoring Centers

This is the core of the digital repressive architecture — official structures operating under names such as Traffic Monitoring Center, Information Security Center, or Operational Communications Control System. They provide:

- interception hubs — backbone points for intercepting internet traffic at major telecom operators;
- DPI systems (deep packet inspection) — real-time traffic decryption and filtering, analysis of VPN, TOR, and messaging platforms;
- social media monitoring — collection of data from public and partially closed platforms;
- messenger analysis — Telegram, WhatsApp, Signal, Viber, and regional applications;
- integration with providers — access to metadata, IP history, geolocation, and communications content.

These centers are built in the style of SIGINT complexes, similar to those in China and Iran. DPI allows not only reading traffic but also preventing communication — blocking VPNs, filtering links, and shaping information flows. The state receives data faster than a user can delete it.

3.2. Commercial Spyware Platforms

When state monitoring is insufficient, commercial solutions are deployed — originally developed for counterterrorism but systematically used against political, business, and media targets.

Common platforms include:

- FinFisher — device compromise, keylogging, access to camera/microphone;
- Pegasus-type solutions — remote infiltration via zero-click attacks, interception of messages and calls;
- Predator/Cytrox, Intellexa — full smartphone takeover, data extraction, copying encryption keys;
- Candiru — intrusion via documents, links, and drive-by malicious code;
- local analogues — tools developed in Russia, Kazakhstan, Azerbaijan, adapted for internal security agencies (MIA/KNB/FSB).

Commercial spyware is more dangerous than classic intelligence tools because it scales: a single package can simultaneously monitor a journalist, an entrepreneur, a member of parliament, and their families. For domestic security agencies, this becomes an industry.

3.3. Illegal Criminal-Hybrid Systems

The third layer consists of informal infrastructure connected to criminal networks collaborating with corrupt security officials. These actors operate outside the law but often gain access to state data systems.

Functions include:

- spyware networks of criminal groups — used to hack businessmen and rivals;
- digital extortion — theft of data followed by demands for business shares, assets, or loyalty;
- shadow monitoring of entrepreneurs — tracking transactions, crypto wallets, movements;
- illegal "surveillance for hire," including selling access to DPI modules and eSIM tracking.

This layer is the bridge between the state and the shadow economy. It allows security agencies to act through "black contractors," maintaining formal deniability.

3.4. Integration With Security and Enforcement Agencies

The final stage in the architecture is the operational use of collected data for pressure, persecution, and coercive governance. Information becomes a tool for:

- access to databases of police, migration, and tax authorities, including phone number histories, banking transactions, and border crossings;
- interception and recording of phone and VoIP calls for later use in criminal cases;
- digital tracking of movements via telecom billing, airports, and Smart Border systems;
- operations through diplomatic channels — extradition requests, Interpol Abuse, cross-border surveillance of refugees;

- persecution of relatives in the home country to pressure those who fled abroad.

The result is a closed-loop system: data collection → analysis → operational deployment → repression. Political control becomes continuous and self-reinforcing.

4. Geography of Digital Surveillance

The digital control infrastructure across Eurasia is uneven, but in most countries a stable model has already formed: the state builds the basic SIGINT framework (traffic interception, DPI, device registration), and around it emerge commercial spyware operators and criminal digital networks. Surveillance covers not only political activists but also large and small businesses, emigrant communities, and the media sector.

4.1. Russia

Russia has one of the most technologically advanced digital surveillance systems in the post-Soviet space. The latest-generation SORM infrastructure effectively enables:

- interception of internet traffic and metadata in real time,
- access to devices without court orders,
- tracking of VPN, TOR, and alternative encryption channels,
- filtering of social media and decryption of messenger data.

SORM 3.0 is integrated with major telecom operators and internet service providers and is used not only for political surveillance but also for monitoring entrepreneurs, anti-corruption investigators, and witnesses in economic cases. Digital channels track contacts with lawyers, cross-border movements, and cryptocurrency operations.

4.2. Kazakhstan

Kazakhstan is rapidly expanding its digital surveillance capabilities following the political crises of 2022. Authorities have gained direct access to:

- telecom operators’ data,
- call and SMS traffic,
- subscriber geolocation and devices,
- connection history for online services.

Pegasus-like spyware is documented in corporate conflicts, where digital hacking is used as frequently as criminal prosecutions and raiding schemes. Female partners of targeted businessmen often become “digital targets” to exert pressure — through phone intrusions, personal correspondence, children’s data, and banking information.

4.3. Azerbaijan

Azerbaijan is one of the regional leaders in the use of commercial spyware systems. Investigations by Amnesty Tech and Citizen Lab have documented large-scale operations against:

- journalists and human rights defenders,

- activists and political migrants,
- entrepreneurs involved in corporate disputes.

Many attacks target individuals abroad — members of the diaspora, asylum seekers, and participants in European investigations. Techniques include hacking Telegram accounts, stealing photos and archives, digital blackmail campaigns, and leaks of "intimate materials" as instruments of repression.

4.4. Uzbekistan and Kyrgyzstan

Here, the infrastructure is less centralized but more hybrid. Mass wiretapping and DPI function alongside criminal spyware networks that often collaborate with security officials.

Key features:

- high-risk P2P operators,
- access to devices of businessmen and lawyers,
- digital attacks during corporate takeovers,
- pressure on migrants residing in the EU or Russia.

Traffic and communications may be monitored not only by intelligence agencies but also by shadow groups purchasing access from mid-level officials.

4.5. South Caucasus (Georgia, Armenia, partially Abkhazia and NK/Artsakh)

The South Caucasus is becoming a transit hub for digital surveillance. The region hosts an emerging infrastructure built around Telegram networks, private intelligence contractors, and P2P operators who sell access to data for cryptocurrency.

Key factors:

- monitoring of entrepreneurs and political opponents,
- attacks on financial and cryptocurrency wallets,
- harassment of female witnesses and partners of business targets,
- cross-border transfer of leaked data to Russia, Azerbaijan, and Turkey.

Unlike Russia and Kazakhstan, the architecture here is less state-driven and more commercial-contractor–based, making it unpredictable and difficult to trace.

5. Transnational Digital Surveillance Operations

Digital surveillance systems in authoritarian states have ceased to be merely tools of domestic control. In recent years, they have evolved into instruments of foreign-policy pressure — regimes now deploy spyware, data interception, and commercial analytical platforms beyond their own borders, tracking the movements of refugees, entrepreneurs, whistleblowers, and political opponents residing in the EU, the US, Turkey, the UAE, and other jurisdictions.

These operations allow governments to intrude into the private lives of individuals under international protection, influence economic assets abroad, and use family members remaining in the home country as hostages for coercion.

5.1. Surveillance of Refugees Abroad

One of the key directions of transnational digital control is monitoring individuals who left their country due to political persecution, economic pressure, or fabricated criminal charges. Methods include:

- interception of phone calls and geolocation analysis,
- covert deployment of spyware on smartphones,
- access to cloud storage, correspondence, archives, and documents,
- automated data collection through banking and passport APIs,
- tracking communications with lawyers, NGOs, and political organizations.

Authorities most often target people who have been granted asylum or hold applicant status — with the aim of forcing them to return, extracting testimony, freezing assets, or silencing them. A common tactic: hacking the victim's phone abroad combined with pressure on relatives who remain in the country. Female partners, parents, and children are used as direct leverage points.

5.2. Corporate Digital Harassment

Spyware is used not only for political repression but also as a tool in corporate conflicts. In kleptocratic and security-dominated systems where business and the state are intertwined, digital attacks function as mechanisms for judicial pressure, hostile takeovers, and asset confiscation:

- targeted hacking of devices belonging to top managers, founders, and accounting departments,
- theft of contracts, confidential deals, and trade secrets,
- fabrication of correspondence for future criminal prosecution,
- leaks of personal photos, audio, and messages to discredit targets,
- attacks on lawyers, journalists, and case witnesses.

Digital surveillance has become the first stage of a raider takeover — preceding asset freezes, searches, criminal proceedings, and the issuance of Interpol Notices.

5.3. Political Operations Outside the Country of Origin

Authoritarian states increasingly use digital surveillance to persecute political opponents living abroad. Documented cases include monitoring political migrants in Europe, tracking protest participants within diasporas, and attempts to identify individuals who fund opposition movements or cooperate with international NGOs.

Main methods:

- collecting data on meetings and travel via device tracking,
- digitally recording contacts with diplomats, journalists, and international bodies,
- discreditation through media leaks, publication of intimate correspondence, and deepfake materials,
- cyberattacks prior to international speeches, conferences, and rallies,
- targeted campaigns aimed at damaging reputations in host countries.

Transnational digital surveillance has become a tool for maintaining political control despite emigration and is emerging as a distinct component of hybrid foreign policy.

6. Case Studies

Case 1 — Spyware Used Against an Entrepreneur

In 2023, an entrepreneur from a Central Asian country, involved in a corporate dispute with his partners, noticed suspicious activity on his phone: rapid battery drain, spontaneous network connections, and unknown processes running in the background. A forensic analysis later confirmed the presence of a commercial spyware module similar in architecture to Pegasus-type platforms.

The data transmitted to the attackers included:

- access to banking applications and corporate accounts,
- transaction history, correspondence with lawyers, contracts,
- geolocation and records of meetings with potential investors.

A few weeks after the infection, an Interpol notice was initiated on the basis of an "economic crime" that had not previously existed in the legal proceedings. Simultaneously, the entrepreneur's assets in his home country were frozen, and pressure was applied to his wife and relatives.

Spyware became the first phase of the operation: **data collection → criminal case initiation → Interpol Notice → attempted extradition.**

Case 2 — Digital Attack on a Whistleblower

In 2024, a former employee of a major state entity provided international media outlets with evidence of corruption schemes related to financial flows in export projects. Within days, her devices were subjected to a targeted hack: covert activation of the camera, extraction of messenger data, and monitoring of her contacts were detected.

The attack involved:

- interception of her communications with journalists and lawyers,
- attempts to access cloud archives,
- mapping of her personal network within the EU,
- threats delivered via anonymous Telegram channels.

Following the digital intrusion came a psychological pressure phase: private photos and messages were leaked online, articles appeared on anonymous media platforms, and her public reputation was systematically attacked.

The goal was not physical harm, but **to erode trust, discredit her, and sabotage future testimony.**

Case 3 — Corporate Conflict with a Digital Phase

In 2025, a dispute between two major holdings escalated from an economic disagreement into a forceful digital confrontation. Initially, the parties exchanged legal claims, but after negotiations failed, one side initiated a spyware operation.

The scheme developed in several stages:

1. **Spyware deployment via corporate email.**

   A malicious attachment disguised as partner documentation enabled access to internal correspondence and archives.

2. **Theft of commercial data.**

   Extracted materials included project files, contracts, tender documentation, pricing models, and strategic presentations.

3. **Compromise phase:**

   Some of the information was leaked to "dump" media platforms, while other portions were used to pressure international banking partners.

4. **Information attack:**

   Selectively manipulated fragments of correspondence were published to create the impression of a "criminal narrative."

This case demonstrated that spyware has become an instrument of corporate competition as much as a mechanism of political persecution. The digital phase of the conflict altered the economic balance between the parties far more significantly than traditional legal methods.

7. International Risks

1. Threat to Diplomatic and Human Rights Structures

Digital surveillance operations undermine the work of international human rights organizations, lawyers, journalists, refugee-assistance structures, and UN/EU human rights missions.

Intercepting correspondence, monitoring communication channels, hacking devices, and tracking movements make confidentiality of protection practically impossible. In several documented cases, access to privileged lawyer–client communication was obtained *before* a complaint was filed with the ECtHR or the UN Working Group on Arbitrary Detention, allowing the state to prepare a counter-dossier in advance, influence the court's position, and discredit the victim.

Thus, spyware becomes a tool of pre-emptive neutralization, violating the principle of independence of international procedures.

2. Pressure on Applicants to International Courts

Digital surveillance affects access to fair judicial process and the ability of individuals to seek protection.

When a politically or economically persecuted person files a complaint with the ECtHR, WGAD, UN CAT, or the Inter-American Commission, their devices become targets of targeted exploitation.

Consequences include:

- monitoring of communications with lawyers, journalists, and witnesses;
- access to drafts of complaints and evidence;
- subsequent pressure on relatives and children.

As a result, the very act of seeking international protection may intensify persecution, creating a chilling effect and reducing the number of applicants willing to fight for their rights.

3. Criminalization of Digital Technologies

Commercial spyware platforms originally designed to combat terrorism and crime are now used as tools of political and corporate repression.

States deploy FinFisher/Predator/Pegasus-class services, while criminal groups simultaneously acquire access to zero-day exploits, SIM-injection tools, and remote data interception.

This generates a shadow market of digital intelligence, where boundaries between state actors and criminals disappear, and surveillance technologies become globally traded illicit assets.

4. Systematic Human Rights Violations

Mass surveillance and targeted spyware operations systematically infringe rights protected by the European Convention on Human Rights:

- **Art. 3** — prohibition of inhuman treatment, including psychological pressure through surveillance and digital extortion;
- **Art. 6** — violation of the right to a fair trial when lawyer–client communications are hacked;
- **Art. 8** — interference with private and family life via location tracking and communication monitoring;
- **Art. 10** — restriction of freedom of expression through blackmail, threats, and publication of stolen data.

Spyware undermines the foundations of international legal order — access to justice, personal autonomy, data security, and digital freedom.

5. Undermining International Security

The export of digital surveillance technologies has become as significant a source of risk as the export of weapons.

Authoritarian states disseminate spyware, train foreign operators, and support digital operations in third countries, influencing politics, elections, business conflicts, and migration processes.

This creates a new class of threats:

- transnational digital attacks against politicians and journalists abroad,
- interference in corporate deals and public procurement,
- formation of international spyware alliances.

Digital surveillance is no longer an internal issue — it has evolved into an instrument of foreign policy coercion and exported repression, directly affecting the architecture of international security.

8. Forecast 2025–2027

1. Growth of Spyware Operations via Telegram and WhatsApp

Between 2025 and 2027, attacks are expected to scale not through SMS infections or phishing emails, but through built-in messenger infections, exploits inside VoIP calls, video previews, and file-preview mechanisms.

Telegram, WhatsApp, and Signal will become not only delivery channels for malicious code, but also platforms for botnet management, surveillance orchestration, and remote interception.

Most likely vectors of evolution:

- exploitation of zero-click vulnerabilities;
- injection through Telegram bots, forwarded channels, and cloud storage;
- interception of chats and voice messages without physical access to the device.

Surveillance will become nearly invisible, and the volume of data collected by security agencies will expand dramatically.

2. Spread of Predator-like Systems in the CIS

Predator, Cytrox, and Candiru-class spyware — previously observed mainly in the Middle East and North Africa — will spread widely across Eurasia. Reasons:

- emergence of local integrators trained by foreign vendors;
- high demand for covert monitoring of entrepreneurs and politicians;
- falling prices of spyware licenses.

By 2027, at least 6–8 CIS and Caucasus states may gain access to platforms capable of:

- intercepting calls,
- extracting cloud data,
- decrypting Telegram chats,
- activating cameras and microphones without notification.

Spyware will become a norm rather than an exception.

3. Intensification of International Investigations

Amid rising digital operations targeting emigrants and human rights defenders, an expansion is expected in:

- the EU Parliament *Pegasus Inquiry*;
- joint Europol + Eurojust operations;
- initiatives of UN Special Rapporteurs on digital violence;
- transnational investigative journalism (OCCRP, *Der Spiegel*, *Le Monde*, *The Guardian*).

The probability of active global cooperation will increase, but so will counterpressure — CIS states will block requests, conceal contracts, and develop local spyware analogues.

The confrontation will evolve into a technology race.

4. New EU Standards in Digital Law

By 2026–2027, the EU will form a new regulatory architecture of digital oversight and protection, expanded after the adoption of the AI Act and the NIS2 reform.

Expected measures:

- criminal liability for spyware use without a judicial mandate;
- mandatory notifications of digital interception akin to wiretap rules;
- legal prohibition on exporting spyware to authoritarian regimes;
- a unified EU audit system for cyber products and vendor monitoring.

If implemented, a portion of attacks will shift from Europe to the CIS, the Middle East, and Africa — regions with weaker human-rights protections.

5. Growth of Interpol Abuse Combined with Digital Pressure

Digital surveillance and Interpol Red Notices will increasingly be used as a single integrated pressure mechanism.

Typical model:

1. data collection through spyware,
2. fabrication of evidence,
3. issuance of an international arrest warrant,
4. attempted extradition combined with pressure on the family.

By 2027, such cases may increase by 30–50%, especially against entrepreneurs, whistleblowers, dissident officials, and political–economic refugees.

For the first time, digital persecution evolves into an international legal weapon, merged with Interpol’s institutional mechanisms.

9. ARGA Observatory Recommendations

For international institutions and supranational organizations

A global mechanism for overseeing digital surveillance systems is urgently required — one comparable in scale to existing arms-control regimes. Surveillance technologies now perform the same strategic functions as weapons: they restrict freedoms, create security risks, and serve as instruments of political coercion.

The first priority is the creation of an international registry of spyware operators and interception-system suppliers, including software developers, integrators, license brokers, and governmental clients.

Such a registry should operate similarly to an Export Control List: every transaction, lease, and technical deployment must be recorded, and all exports of surveillance technologies must be subject to sanctions oversight and legal control.

The second key mechanism is the monitoring of digital threats against applicants for international protection, particularly entrepreneurs, whistleblowers, and political refugees. International human-rights bodies must respond not only to physical pressure, but also to digital attacks — device intrusions, communication interception, and targeted disinformation or smear campaigns.

The third direction is the integration of digital evidence into international judicial processes. By 2027, it is feasible to establish standards for accepting digital logs, network traces, forensic reports, and cryptographic chains as admissible evidence of intelligence-service interference. This would enable courts to formally recognize digital persecution as a form of coercion and, in some cases, psychological torture.

For the EU, the United States, and the United Kingdom

Western regulators have begun to build sanctioning frameworks against spyware exporters, but the system remains fragmented. A shift toward a unified sanctions regime is required — one that encompasses:

- developers of spyware platforms,
- system integrators,
- licensing intermediaries,
- and state importers who use these systems for torture or political repression.

Export-control restrictions must be embedded into the architecture of GDPR, the AI Act, DSA/DMA, and forthcoming digital-autonomy regulations. The export of any surveillance module to an authoritarian jurisdiction should automatically trigger a sanctions procedure.

The next step is mandatory reporting on spyware infrastructure, similar to ESG disclosures. Technology companies, telecom operators, and cloud platforms should be required to publish information on any cooperation with digital-surveillance entities, including the supply of equipment, DPI systems, and interception technologies.

For academic and research institutions

Leading universities and analytical centers have been slow to react to the evolution of digital authoritarian tools. There is a pressing need to institutionalize a field of study called Digital Surveillance Criminology — a discipline at the intersection of cybersecurity, international law, digital criminology, and political anthropology.

This field should include:

- analysis of spyware ecosystems as systems of transnational violence,
- study of corporate and governmental models of digital control,
- statistical documentation of attacks on activists, refugees, and business emigrants,
- development of a database of digital intrusions correlated with Interpol Abuse, political repression, and corporate conflicts.

Building a centralized archive of digital attacks would provide an objective evidentiary foundation for future international investigations, court proceedings, sanctions packages, and United Nations reports.

10. Conclusion

Digital surveillance has ceased to be an auxiliary tool of repression and has transformed into an independent political resource shaping the architecture of power in authoritarian regimes. Across Eurasia, surveillance technologies have become not merely an addition to classical intelligence agencies but the core of a new mechanism for controlling society, business, elite groups, the opposition, migrants, and refugees abroad. The infrastructure of digital monitoring operates transnationally, unconstrained by state borders, and creates a threat to international security on a scale comparable to weapons systems and financial pressure.

This report demonstrates that digital control functions as a complex, multi-layered system that includes state monitoring centers, commercial spyware products, illegal hybrid criminal networks, and infrastructure embedded within the security apparatus. These technologies do not merely collect data; they create mechanisms of influence: they are used to persecute entrepreneurs, pressure partners and relatives of targeted individuals, manipulate diaspora communities, and obstruct access to justice through fear, surveillance, and digital coercion.

Digital repression has become autonomous: it operates around the clock, requires no physical presence, leaves no direct traces, and is therefore harder to detect and more difficult to stop. States can exert pressure on individuals located abroad or under international protection, meaning that traditional legal safeguards are no longer sufficient. This demands a rethinking of international-law paradigms, the integration of digital evidence into judicial processes, and the creation of monitoring structures comparable in scale to arms-control mechanisms.

ARGA Observatory's report provides an analytical basis for understanding digital authoritarianism as a global challenge. It proposes viewing spyware infrastructures not as internal security tools of states but as international factors that threaten human rights, the rule of law, and the stability of global systems. The next step is to develop supranational regulatory instruments, a global registry of spyware operators, sanctions mechanisms, legal protections for applicants, and an academic discipline specializing in digital coercion.

Digital surveillance is thus a new form of power, a new layer of geopolitics, and a new domain of international regulation. The future of security will be defined not by who controls territories and armies, but by who controls data, communication infrastructure, and the digital presence of individuals online. ARGA Observatory identifies the beginning of this era and establishes the foundation for developing international responses.

Sources

1. GIJN, Madeline Earp, Pegasus Project Reveals Addes Risks for Corruption Reporters, August 13, 2021, https://gijn.org/stories/pegasus-project-reveals-added-risks-for-corruption-reporters/.
2. OCCRP, Israeli-Made Spyware Used to Monitor Journalists and Activists Worldwide, July 18, 2021, https://www.occrp.org/en/project/the-pegasus-project/israeli-made-spyware-used-to-monitor-journalists-and-activists-worldwide.

3. Lighthouse Reports, Haaretz, Flight of the Predator, November 30, 2022, https://www.lighthousereports.com/investigation/flight-of-the-predator/.
4. Econstor, Fredrik Erixon, Hosuk Lee-Makiyama, Digital authoritarianism : Human rigths, geopolitics and commerce, 2011, https://www.econstor.eu/bitstream/10419/174715/1/ecipe-op-2011-5.pdf.
5. IPHR, Russia's Digital Authoritarianism : The Kremlin's Toolkit, https://iphronline.org/wp-content/uploads/2023/12/digital-authoritarianism-report.pdf.
6. HRW, Maya Wang, China's Techno-Authoritarianism Has Gone Global, April 8, 2021, https://www.hrw.org/news/2021/04/08/chinas-techno-authoritarianism-has-gone-global.
7. ECHR, Mass surveillance, June 2024, https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng.
8. EDPS, Preliminary Remarks on Modern Spyware, 15 February 2022, https://www.edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en.
9. OHCHR, Special Rapporteur on the right to privacy, https://www.ohchr.org/en/special-procedures/sr-privacy.
10. Privacy International, Private Interests : Monitoring Central Asia, November 2014, https://privacyinternational.org/sites/default/files/2017-12/Private%20Interests%20with%20annex_0.pdf.
11. OONI, Kazakhstan : TLS MITM attacks and blocking of news media, human rights, and circumvention tool sites, https://ooni.org/post/2024-kazakhstan-report/.
12. Parliamentary Assembly, Pegasus and similar spyware and secret state surveillance, 20 September 2023, https://rm.coe.int/pegasus-and-similar-spyware-and-secret-state-surveillance/1680ac7f68.