Policymaking and Institutional Mapping of Surveillance and Interception on Citizens under the Islamic Republic of Iran

Part 4: Transnational Proliferation of Surveillance, Interception, and Control Tech

Privacy Rights and Surveillance Monitoring (PRISM)
Holistic Resilience, Inc., December 2025

Policymaking and Institutional Mapping of "Surveillance and Interception" on Citizens under the Islamic Republic of Iran

***

Part 4: Transnational Proliferation of Surveillance, Interception, and Control Technology

---

This report explores how the Islamic Republic of Iran exports its surveillance, interception, and digital control technologies to allied states and foreign partners. It examines the transnational networks, commercial intermediaries, and diplomatic strategies used to proliferate censorship tools, spyware, and telecom monitoring infrastructure. The analysis highlights how authoritarian tech diffusion is not incidental, but an intentional extension of Iran's domestic surveillance model onto the global stage.

December 2025

Privacy Rights and Surveillance Monitoring (PRISM)

***

Holistic Resilience

Abstract

Policymaking and Institutional Mapping of "Surveillance and Interception" on Citizens under the Islamic Republic of Iran; Part 4: Transnational Proliferation of Surveillance, Interception, and Control Tech

This report investigates the structures, actors, and evidence surrounding the Islamic Republic of Iran's efforts to export internet repression technologies. Drawing on official documents, cybersecurity disclosures, and credible international reports, it demonstrates that the Islamic Republic has not only expanded its domestic arsenal of surveillance, censorship, and information control technologies, but has also developed institutional and diplomatic frameworks to offer these systems to other states.

Building upon Policymaking and Institutional Mapping of "Surveillance and Interception" on Citizens under the Islamic Republic of Iran; Part 1: Surveillance Governance and Infrastructures for Interception and Data Access, this second part begins by analyzing strategic partnerships with China and Russia; two countries that, through long-term agreements, have facilitated the transfer of surveillance technologies and the advancement of state-centric internet governance models. It then examines the role of Iranian private and semi-governmental companies in developing filtering systems and Deep Packet Inspection (DPI) tools, and presents documentation of diplomatic support for these companies through platforms such as the "Knowledge-Based Export Companies Club" (IHTECC).

Further sections explore sanction-evasion mechanisms, the role of intermediary firms in the UAE, Turkey, and other jurisdictions, and the covert transfer of dual-use technologies. The report also highlights the risk posed by initiatives like the "Iran House of Innovation and Technology" (IHIT), which may be repurposed as fronts for the export of sensitive technologies.

In its conclusion, while emphasizing the absence of explicit evidence for direct exports of full-spectrum censorship infrastructure such as the technical capabilities behind the National Information Network (NIN) to autoritarien countries, the report warns that the potential for such transfers is significant and

largely substantiated by indirect and OSINT-based findings. It argues that addressing this transnational threat demands greater transparency, continuous monitoring, and advanced investigative research.

Privacy Rights and Surveillance Monitoring (PRISM)

Holistic Resilience, Inc.

December 2025

Table of Contents

Glossary of Abbreviations

Acronyms:	Full Term:

Islamic Republic of Iran Bodies:

CRA	Communications Regulatory Authority
FARAJA	Islamic Republic of Iran's Law Enforcement Forces; Police
FATA	Islamic Republic of Iran's Cyber Police
IRGC	Islamic Revolutionary Guard Corps
IRGC-IO	IRGC Intelligence Organization
ITO	Information Technology Organization of Iran
MIMT	Ministry of Industry, Mine and Trade
Ministry of ICT	Ministry of Information and Communications Technology
MOIS	Ministry of Intelligence
NCC	National Center for Cyberspace
NIN	National Information Network
NOCR	National Organization for Civil Registration of Iran
SCC	Supreme Council of Cyberspace
SCCR	Supreme Council of Cultural revolution
SCNS	Supreme Council of National Security
TCI	Telecommunication Company of Iran
TIC	Telecommunication Infrastructure Company

State-Controlled Surveillance and Interception Systems:

EMTA	E-commerce Customer Authentication System
HAMTA	Smart System of Communication Devices Registry
HODA	Iranian Digital Identity Authentication System
SAMAVA	National Identity and Verification Gateway
SANA	Online Judicial Authentication System
SHAHKAR	Users Authentication Network
SHAMSA	National lawful intercept data archive system
SIAM	Integrated System for Telecommunication Inquiries

General and Technical Terms:

AAA	Authentication, Authorization, Accounting
API	Application Programming Interface
APT	Advanced Persistent Threat
ETSI	European Telecommunications Standards Institute
IMEI	International Mobile Equipment Identity

IMSI	International Mobile Subscriber Identity
ISP	Internet Service Provider
MITM	Man-in-the-Middle
SSO	Single Sign-On
TTPs	Tactics, Techniques, Procedures
VPN	Virtual Private Network
3GPP	3rd Generation Partnership Project

Islamic Republic of Iran Groundplay and Main Actors

Global Proliferation of Surveillance, Interception, Censorship, and Internet Control Technologies

The Islamic Republic of Iran has a long-standing record of leveraging technology to control its domestic information space and suppress dissent (see PRISM Part 1). This strategy, marked by the development of national infrastructures such as NIN and the enforcement of extensive internet censorship, has evolved in recent years with increased complexity and broader scope.[1] Simultaneously, the Islamic Republic has sought to expand its influence on the global stage by forging strategic alliances and securing presence in international decision-making forums. This aspiration was embedded from the outset of the Islamic Republic of Iran's internet governance: in 1998, Supreme Leader Ali Khamenei issued a seven-point directive titled "General Policies for Digital Information Networks," which explicitly included the following:[2]

> *Clause 7: Take appropriate steps to achieve international treaties and regulations and to establish information-sharing alliances with other countries, especially Islamic nations, in order to create balance in the global information sphere and to preserve national identity and culture while resisting global domination.*

These dual trajectories, domestic control and foreign influence, intersect at the point of exporting internet surveillance and control technologies. As a means to resist international pressure and advance its regional and global agendas, the Islamic Republic has deepened its cooperation with aligned states, particularly China and Russia. These partnerships span economic, military, intelligence, and technological domains, creating a fertile environment for the exchange of expertise and equipment, including tools for cyber governance, censorship, and digital surveillance.

---

[1] Freedom House; "Freedom Net 2024"; Jun 2024; Link, Archive

[2] Ali Khamenei, The Supreme Leader of the Islamic Republic of Iran; "General Policies for Digital Information Networks"; Oct 1, 1998; Google Translated Link, Archive

Strategic Foundations and Motivations for Export

Long-term strategic and security agreements of the ISlamic Republic of Iran with powers such as China and Russia have created favorable conditions for the exchange of technologies across a range of domains from digital surveillance and cybersecurity to offensive cyber capabilities. The 25-year agreement with China,[3] which encompasses economic, military, and cyber cooperation, explicitly references the transfer of technologies applicable to internal control and monitoring mechanisms:[4]

> *Annex 1 of the agreement, under its list of primary objectives, calls for deepened collaboration in the field of information and communications technologies, specifically naming "various aspects of cyberspace and end-user equipment."*
>
> *Annex 2, outlining the main areas of comprehensive 25-year cooperation, includes the following in Clause D: cooperation on telecommunications technology, the development of fifth-generation (5G) infrastructure, core services (search engines, email, and social messaging platforms), telecommunications hardware (GPS routers, switches, servers, and data storage systems), end-user devices (mobile phones, tablets, and laptops), operating systems for both computers and mobile devices, antivirus software, and artificial intelligence.*

Reports suggest that China has supported the Islamic Republic in enhancing its internet censorship infrastructure, with Chinese companies such as ZTE and Huawei playing active roles in selling surveillance systems used to monitor landline, mobile, and internet communications, as well as in expanding the country's communications infrastructure.[5] These collaborations, situated within the framework of China's Belt and Road Initiative (BRI), have

---

[3] "Iran-China Comprehensive Cooperation Plan (25 Years)", Unconfirmed text; Jun 2020; Download

[4] Ghazal Vaisi; Middle East Institute; "The 25-year Iran-China agreement, endangering 2,500 years of heritage"; Mar. 1, 2022; Link, Archive

[5] Tehran Bureau; "The Chinese Companies Building Iran's Surveillance State"; Sep. 30, 2022; Link, Archive

raised alarm over the Islamic Republic's emulation of the Chinese model of internet control particularly the Great Firewall of China and its potential use of similar technologies to suppress dissent.[6]

Similarly, the Comprehensive Strategic Agreement (Security; 2025)[7] and the Bilateral Agreement on Information Security (Cybersecurity; 2021)[8] between the Islamic Republic of Iran and Russia emphasizes cooperation in the areas of cybersecurity, the fight against cybercrime, and the exchange of expertise related to national internet governance.[9]

The security agreement calls for enhanced collaboration between Iranian and Russian intelligence and security institutions for the exchange of data and operational experience, stating: "The intelligence and security agencies of the Contracting Parties shall cooperate within the framework of separate agreements."

Furthermore, the same agreement formalizes bilateral activities within the framework of the "Agreement on Cooperation in the Field of Information Security." The draft text of this cooperation agreement was leaked in January 2021. It was subsequently ratified by the Iranian Cabinet in July 2022, submitted to Parliament, and officially passed in June 2024.

The agreement underscores joint development and technology exchange initiatives aimed at deploying and strengthening state-controlled, nationally bounded networks in both Iran and Russia. It calls for "enhancing national sovereignty in the international information space,"

---

[6] A Conversation with Nader Habibi and Hadi Kahalzadeh; Crown Center for Middle East Studies, Brandeis University; "The Iranian-Chinese Strategic Partnership: Why Now and What it Means"; Apr 28, 2021; Link, Archive

[7] "Iran-Russia Comprehensive Strategic Agreement"; Jan 2025, download

[8] "Agreement on Cooperation in the Field of Information Security between the Government of the Islamic Republic of Iran and the Government of the Russian Federation"; July 2024; Link, Archive

[9] SC Media; "Increased cybersecurity cooperation forged by Russia, Iran"; Jan. 23, 2025; Link, Archive
Council on Foreign Relations; "The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East"; Mar. 15, 2021; Link, Archive
Emilio Lasiello; Strike Source; What Does Iran-Russia Cyber Partnership Mean for US National Security?"; Feb. 2, 2021; Link, Archive

countering “attempts to limit sovereign rights to regulate and secure national segments of the global network,” and sharing best practices for “managing national internet segments and developing infrastructure” all of which pertain directly to systems analogous to those developed by the Islamic Republic of Iran for the surveillance and interception of its own citizens.

The cybersecurity agreement outlines specific details of this cooperation. The agreement enumerates six shared information security threats, including the dissemination of propaganda content deemed harmful to the “social, political, economic systems, and the spiritual and moral environment” of the contracting states.

The cybersecurity agreement provides a legal framework for the exchange of necessary technologies, technical assistance, and international collaboration to overcome the threats outlined. This agreement implicitly facilitates the sharing of tools, methods, and operational experiences related to surveillance and interception of citizens’ private lives. The agreement thus establishes a bilateral mechanism for the export of technologies that enable repression and digital espionage.

Both countries share strategic interests in promoting state-centric models of internet governance and in resisting what they describe as “Western influence.” Russia has actively supported the cybersecurity apparatus of the Islamic Republic of Iran, and Russian technology companies including sanctioned entities such as Positive Technologies have engaged in meetings with Iran’s Ministry of ICT regarding the export of Russian technology and bilateral cooperation in cybersecurity and telecommunications.[10]

[10] Darya Lavrova; Positive Technologies; “Iran's cybersecurity threatscape for 2021–H1 2024”; Oct 25, 2024; Link, Archive
Jazeh Miller; Iran News Update; “Iran’s Regime Tightens Grip on Internet Access through Cyber Partnership with Russia”; Jan. 23, 2025; Link, Archive

Russia's pursuit of a sovereign "independent internet" and the Islamic Republic's efforts to complete its National Network (NIN) reflect parallel trajectories toward enhanced state control over internet and digital ecosystems.

Iran's presence in international forums such as the International Telecommunication Union (ITU) also provides a platform to promote its vision of internet sovereignty and challenge more open internet governance models.[11] The Islamic Republic's formal complaint against Starlink at the ITU, along with efforts to compel the company to comply with domestic Iranian regulations, exemplifies its broader push to expand state control over the internet extending state control into domains beyond its sovereign jurisdiction.[12]

Taken together, these agreements, partnerships, and institutional mechanisms form a strategic foundation through which the Islamic Republic not only develops domestic capabilities for internet control and surveillance but also acquires the motive and potential infrastructure to export such technologies and related know-how to aligned states or external clients.

[11] Farzaneh Badii; Digital Medusa; "Islamic Republic V. Starlink: Will The ITU Fragment Satellite Internet?"; Jan. 29. 2024; Link, Archive

[12] Miaan Group; "ITU Must Press Iran on Internet Shutdowns, Not Enable Them"; Aug. 21. 2024; Link, Archive

Iranian Companies and Contractors Exporting Internet Repression Technologies

In addition to top-level state cooperation, commercial mechanisms have emerged to market and export technologies with dual-use or surveillance-related functions. The development and maintenance of the Islamic Republic of Iran's sophisticated censorship and surveillance infrastructure relies on close collaboration between government and security institutions and a network of private and semi-private technology firms. These entities play a pivotal role in localizing, developing, and implementing tools for internet control.

Over the past decade, several Iranian companies have actively engaged in the development and deployment of technologies related to censorship and network control. These include Deep Packet Inspection (DPI) systems, advanced firewalls, and content monitoring platforms, most of which are utilized by the Islamic Republic's security agencies to impose internet restrictions.[13]

An examination of these companies and their product portfolios reveals both the technical capacity of the Islamic Republic in this domain and its potential for export. However, one of the main limiting factors on their international operations has been the imposition of international sanctions. In response to Iran's expanding internet censorship regime and ongoing human rights violations, the United States and the European Union have designated many of these firms and affiliated state institutions.

Nonetheless, these sanctions have not deterred the Islamic Republic's foreign diplomatic apparatus from actively promoting these firms abroad. For example, the Embassy of the Islamic Republic in Paris has circulated promotional catalogs featuring Iranian technology firms

[13] Factnameh; "Iranian Filtering Contractors"; Feb 29, 2023; Link, Archive

across various categories.[14] Among the featured companies are dozens that are either directly sanctioned or belong to holding groups listed under U.S. and EU sanctions.

Douran Software Technologies, Inc.

One example is the sanctioned firm Douran Software Technologies, a key contractor to the Office of the Prosecutor General and the Filtering Committee of the Islamic Republic of Iran, responsible for implementing internet censorship systems.[15] In the promotional materials, the company is listed under the “Information Technology” category, though its legal name is neither accurately nor transparently identified.[16] Douran, along with similar firms, has collaborated closely with security agencies in the Islamic Republic to develop technologies that enable extensive control and monitoring of citizens’ internet activity.

This catalog was produced by the Economic Diplomacy Office of the Ministry of Foreign Affairs of the Islamic Republic of Iran, and it is reasonable to assume that it has been distributed across Iranian embassies particularly in authoritarian or aligned states to promote these companies to potential foreign clients.[17]

The listed companies are part of a group labeled the “Club of Knowledge-Based Export Companies,” whose name appears throughout these catalogs.[18] This “Club” is a joint initiative between the Vice Presidency for Science and Technology and the Ministry of Foreign Affairs of the Islamic Republic of Iran.

---

[14] Embassy of the Islamic Republic of Iran, Paris; "Introduction to Iranian Knowledge-Based Export Companies"; 25 September 1402; Archive

[15] Open Sanctions; “Douran Software Technologies”; Link

[16] IHTECC; “Iran Hi-Tech Export Companies Club, Information technology”; Aug 2022; Link, Archive

[17] Deputy for Economic Diplomacy, Ministry of Foreign Affairs of the Islamic Republic of Iran; "Exemplary Export Companies"; Link 1, Link 2

[18] Knowledge-Based Export Companies Club; Link

Amn Afzar Gostar Sharif

Dozens of Iranian entities under international sanctions, many specializing in dual-use technologies are actively promoted on the official website of the Ministry of Foreign Affairs of the Islamic Republic of Iran. One prominent example is Amn Afzar Gostar Sharif, a blacklisted contractor known for developing surveillance and filtering systems, whose capabilities are explicitly listed for foreign clients in government-published promotional materials.[19]

[19] Open Sanction; “Amn Afzar Gostar Sharif”; Link

خانه / شرکت های نمونه صادراتی / دانش بنیان / امن افزار گستر شریف

امن افزار گستر شریف

اطلاعات شرکت

زمینه های فعالیت:

تولید محصولات امنیتی در حوزه ICT مانند:
Pars WAF
Web Application Firewall
Pars Right DLP
Pars Key
Smart Security Token
PASA
ParsGate UTM: شرکت امن افزار گستر شریف با تکیه بر توان و دانش متخصصان خود و به منظور پاسخ گویی به نیازهای امنیتی سازمانهای کشور از سال 1384 شروع به تولید محصول فایروال پارس گیت نموده است. این محصول با بهره گیری ازپیشرفته ترین فناوری های نوین در فایروال های امروزی تولید شده و قابل رقابت با محصولات مطرح دنیا می باشد تولید این محصول در داخل کشور امکان افزودن نیازمندی های خاص سازمان ها و کاربران گوناگون را نیز فراهم ساخته است. پارس گیت یک فایروال بومی برای ارائه مکانیزم های مختلف امنیتی در شبکه های کوچک تا خیلی بزرگ است. این محصول به صورت یکپارچه سرویس های امنیتی متعددی را از قبیل هویت شناسی، حسابرسی مبتنی بر کاربر، بازرسی حالتمند ترافیک، شبکه خصوصی مجازی (VPN)، تشخیص و جلوگیری از حملات شبکه را به همراه واسط های مدیریتی کاربرپسند با دو کانال WUI, CLI ارائه می نماید. امکان مدیریت ساده، انعطاف پذیر و درعین حال قدرتمند سیاست های امنیتی از قابلیت های ویژه این محصول بوده که در کنار سایر ویژگی ها و قابلیت ها پارس گیت را به عنوان یکی از بهترین راه حل های یکپارچه و جامع امنیت شبکه مطرح کرده است.

Leaked documents from the email server of the Islamic Republic's Filtering Committee (the Prosecutor General's Deputy for Internet Affairs) include a letter in which the Prosecutor General's Office nominated nine companies to participate in meetings of the "Open-Ended Working Group on the Security of and in the Use of Information and Communication Technologies (OEWG)," coordinated by the Department for International Peace and Security of the Ministry of Foreign Affairs. Most of the nominated companies are either directly sanctioned or belong to larger conglomerates that are subject to US and EU sanctions.

قوه قضائیه
دادستانی کل کشور
معاونت پیگیری امور فضای مجازی

بسمه تعالی

تاریخ : ۱۴۰۱/۰۲/۳۱
شماره : ۹۰۰۰/۱۳۴۹۷/۱۴۰۱/۴۴۰
پیوست : ندارد

جناب آقای اشراق جهرمی

مدیرکل محترم صلح و امنیت بین المللی وزارت امور خارجه

سلام علیکم

احتراماً بازگشت به نامه شماره ۶۱۵/۱۱۶۹۹۳۵ در تاریخ ۱۴۰۱/۰۲/۲۰ ، برخی سازمان‌ها و مؤسسات غیردولتی داخلی که در حوزه امنیت سایبری فعالیت دارند و در این حوزه صاحب تجربه و تخصص می‌باشند به شرح ذیل جهت مشارکت در جلسات گروه کاری باز امنیت بین‌الملل اطلاعات و ارتباطات، معرفی می گردند:

ردیف	نام و عنوان مؤسسه غیردولتی	حوزه فعالیت	پایگاه اینترنتی
۱	شرکت نرم افزاری امن پرداز (پادویش)	امنیت سایبری و مقابله با بدافزار	www.amnpardaz.com
۲	پژوهشکده امنیت رایاسامانه های شریف	پژوهش در حوزه امنیت سایبری	www.parsasharif.ir
۳	شرکت امن افزار گسترش شریف	امنیت سایبری	www.amnafzar.ir
۴	شرکت اطلاعات و ارتباطات امن مهین	امنیت سایبری	www.mohaymen.ir
۵	دانشگاه صنعتی شریف	امنیت سایبری	www.sharif.edu
۶	شرکت توسعه انفورماتیک فراز پژوهان	امنیت سایبری	www.farazpajohan.com
۷	مرکز تحقیقات صنایع انفورماتیک	امنیت شبکه و فناوری اطلاعات	www.rcii.ir
۸	آزمایشگاه فناوران توسعه امن ناجی	فارنزیک و امنیت سایبری	www.cybersec.ir
۹	شرکت پایش ابزار سیمرغ	امنیت سایبری	

جواد پاپلی
معاون دادستان کل کشور در امور فضای مجازی
و دبیر کارگروه تعیین مصادیق محتوای مجرمانه

رونوشت :

- جناب آقای دکتر سجادی، معاون محترم تنظیم مقررات مرکز ملی فضای مجازی جهت اطلاع.

Iran Innovation and Technology House

Every year, the Supreme Leader of the Islamic Republic of Iran, Ali Khamenei, assigns a name and theme to the new calendar year. This title becomes a key axis of state propaganda and policy alignment across governmental institutions for the entire year. The practice has been a formal tradition for over two decades. When Khamenei designated 1401 (March 2022 to March 2023) as the year of “Production: Knowledge-Based and Entrepreneurship," a range of institutional initiatives were launched to align with the official emphasis on “knowledge-based enterprises.”[20]

One such initiative was the establishment and expansion of the Iran House of Innovation and Technology (IHIT), a state-led program operating under the Vice Presidency for Science and Technology, specifically its Office for the Development of International Scientific and Technological Cooperation.[21] IHIT functions as a global export facilitation network to assist Iranian companies in promoting and selling so-called “knowledge-based technologies.” With branches in Russia, China, Uzbekistan, Turkey, Iraq, Syria, Uganda, and Kenya, IHIT engages in export brokerage and online marketing, creating a potential conduit for the transfer of sensitive technologies including electronics, telecommunications systems, and surveillance-capable infrastructure.

---

[20] Ali Khamenei, The Supreme Leader of the Islamic Republic of Iran; "Nowruz Message on the Occasion of the Beginning of the Year 1401"; Mar 20, 2022; Link, Archive

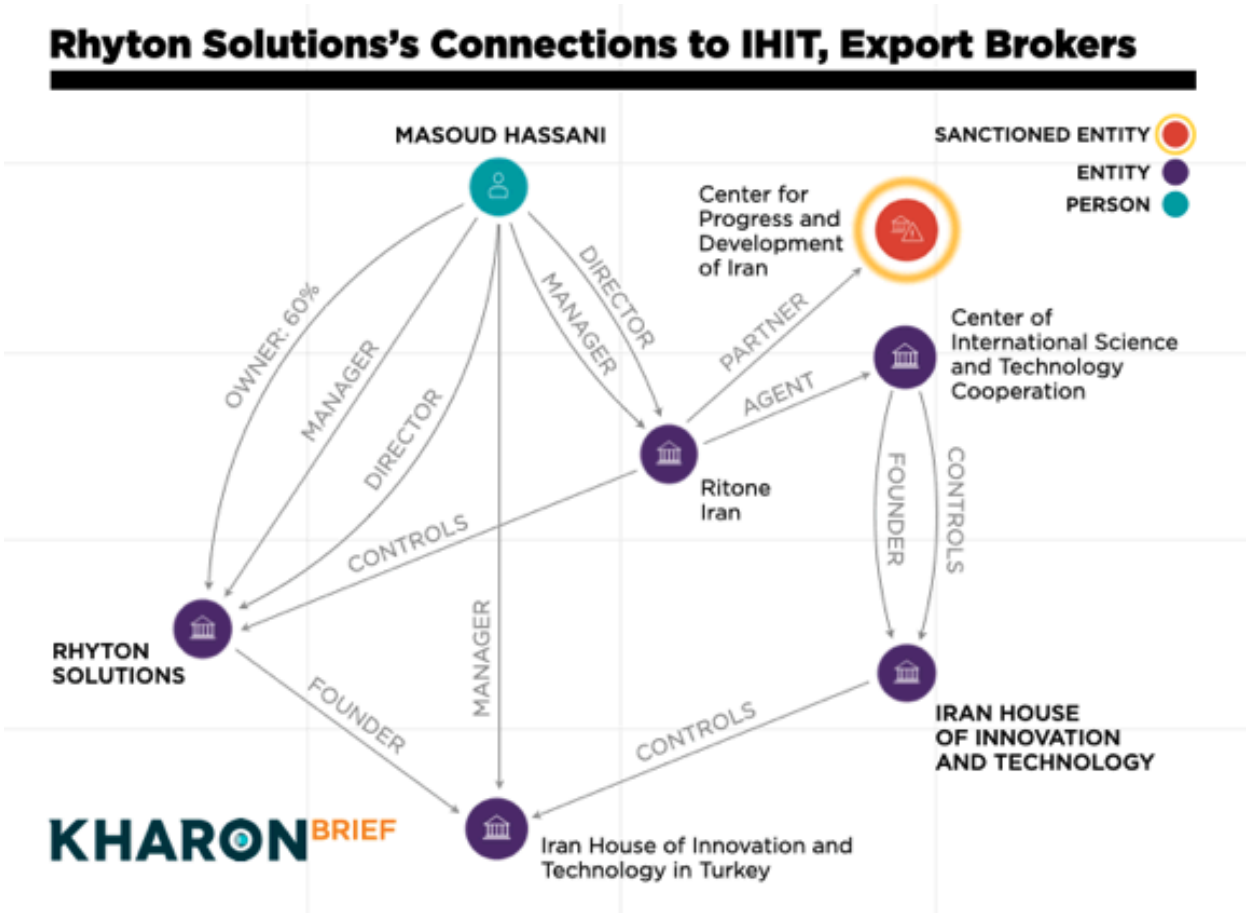
[21] “Iran Innovation and Technology House”; Link 1, Link 2
Organization for the Development of International Scientific and Technological Cooperation, Vice Presidency for Science and Technology of the Islamic Republic of Iran; Link

While the stated purpose of IHIT is to strengthen Iran's knowledge-based economy and circumvent international sanctions, its activities raise credible concerns over the potential for facilitating dual-use exports including technologies with military or repressive applications. A list compiled by another body within the Vice Presidency (Technology Export and Exchange Development Fund) reveals that many of the companies affiliated with IHIT are known contractors and developers of filtering, censorship, and internet repression systems.[22]

IHIT also works closely with private export brokers and Export Management Companies (EMCs). Examples include Amin Development for Technology Export and Exchange, which is IHIT's exclusive representative in Russia; the German-registered Rhyton Solutions GmbH, whose owner is also the director of IHIT's Istanbul office and is linked to the Iranian firm Ritone Iran Inc. (active in tech exports to Russia); and Hirad Smart Trade, a company led by the commercial director of IHIT Russia.[23]

[22] Export Development and Technology Exchange Fund, Organization for the Development of International Scientific and Technological Cooperation; Link

[23] Kharon; "A Sprawling Iranian Network Is Facilitating Its Tech Exports, Sidestepping Sanctions"; Feb 11. 2025; Link, Archive


Rhyton Solutions's Connections to IHIT, Export Brokers
MASOUD HASSANI
SANCTIONED ENTITY
ENTITY
PERSON
Center for Progress and Development of Iran
Center of International Science and Technology Cooperation
Ritone Iran
RHYTON SOLUTIONS
IRAN HOUSE OF INNOVATION AND TECHNOLOGY
Iran House of Innovation and Technology in Turkey
OWNER: 60%
MANAGER
DIRECTOR
MANAGER
DIRECTOR
PARTNER
AGENT
CONTROLS
FOUNDER
CONTROLS
FOUNDER
MANAGER
CONTROLS
KHARON BRIEF

Diplomatic Channels, Sanctions Evasion, and the Global Risk of Exporting Dual-Use Technologies

While the direct role of Iranian embassies in facilitating or marketing internet surveillance and repression technologies is not explicitly documented in the reviewed sources, the Islamic Republic's longstanding approach to leveraging all diplomatic instruments for advancing strategic objectives makes this a plausible avenue warranting further scrutiny.

In 2024, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) implemented new export control measures that restrict the provision of technology services to Iranian state institutions.[24] These regulations established specific standards for hardware that may be legally exported to the Islamic Republic. The European Union has enforced similar human rights-related sanctions since 2011, prohibiting the provision of technical, financial, or brokerage services related to equipment that could be used for internal repression including systems for internet and communications surveillance.

Evidence suggests that the Islamic Republic of Iran relies on a complex network of intermediary companies across multiple jurisdictions to circumvent these sanctions and import dual-use technologies. These networks operate through shell companies, forged documentation, and proxy procurement structures in countries such as the United Arab Emirates, Turkey, Malaysia, Singapore, and China. Several nodes in this web have been publicly exposed.

[24] OFAC; "31 CFR Parts 501 and 515"; Mar. 21, 2025; Link, Archive

In one notable case, in February 2024, OFAC imposed sanctions on four companies and three individuals operating in Iran, the UAE, and Turkey for transferring sensitive US-origin technologies to the Central Bank of Iran.[25] Among the sanctioned entities was the Informatics Services Corporation, Iran's primary state-owned fintech provider and the entity responsible for building infrastructure for the country's planned national cryptocurrency.[26]

A critical component of these export regulations is the designation and control of "cyber-surveillance items" defined as dual-use goods "specifically designed to enable covert surveillance of natural persons by monitoring, extracting, collecting, or analyzing data from information and telecommunications systems." While such export control regimes, particularly from the United States, do impose real costs and barriers to the Islamic Republic's expansion of its internet control infrastructure, enforcement challenges remain. The operational complexity of these networks, the availability of global intermediaries, and the lack of harmonization between jurisdictions significantly undermine the full effectiveness of existing restrictions.

Nevertheless, Iran's strategic alliances and institutional mechanisms reflect a systematic effort to integrate into alternative power structures beyond the Western sphere. These relationships are being leveraged to reinforce domestic capacities particularly in the domain of digital control and to open new pathways for technological exports and influence projection. Its partnerships with China and Russia not only facilitate access to advanced technologies but also underpin a

[25] Fatima Hussein; AP; "U.S. sanctions Iran Central Bank subsidiary for U.S. tech procurement and violating export rules"; Feb. 14, 2024; Link, Archive

[26] Open Sanction; "Informatics Services Corporation"; Link

shared ideological front against open internet models, promoting a vision of state-led “internet sovereignty” as a counterweight to global digital liberalism.

Conclusion and Assessment

Evidence clearly shows that the Islamic Republic of Iran has developed significant and increasingly localized technical capabilities for digital control and surveillance. These include infrastructures such as NIN, advanced systems like SIAM for monitoring mobile communications, widespread deployment of DPI for censorship and VPN blocking, and novel tools of social oversight such as the Nazer app and facial recognition technologies. These capabilities have been extensively used within Iran to suppress dissent and restrict the flow of information and have likely been bolstered through cooperation with China and Russia.

Externally, the establishment of institutional frameworks such as IHIT reflects a clear intention to export these technologies including dual-use systems and circumvent international sanctions. Strategic alignments with China and Russia further emphasize shared interests in promoting alternative internet governance models and resisting Western influence.

Despite the Islamic Republic’s technical capabilities and apparent intent, the available body of evidence reviewed in this report does not contain verified documentation of systematic exports of core censorship or surveillance infrastructures such as components of the NIN or SIAM to aligned states like Venezuela. What exists is largely indirect, circumstantial, or OSINT-based. This stands in sharp contrast to the well-documented export of Iranian military technologies

such as drones and missiles to Russia and proxy forces, indicating that the Islamic Republic's efforts to export surveillance, interception, and information control technologies have so far received less international scrutiny.

Nonetheless, the Islamic Republic's actions including the expansion of NIN, its challenge to Starlink at ITU, and its deepening alliances with China and Russia contribute to the accelerating global trend of internet fragmentation and the rise of state-centric "internet sovereignty" models. These developments threaten the open and global internet paradigm and aid in the proliferation of authoritarian digital governance.

Given Islamic Republic of Iran's demonstrated technical capacity, existing export infrastructure, and the clear strategic interest in promoting its model abroad, the risk of such exports is real and credible. This calls for sustained monitoring, deeper investigative efforts, and heightened international vigilance to trace, document, and counter the potential global dissemination of Iranian-built digital repression tools. The current lack of definitive evidence should not be misconstrued as the absence of threat; rather, it must serve as an impetus for intensified transparency and oversight initiatives.