MIAAN GROUP

Internet Oppressors

A Look at the Office of Iran’s Attorney General and its Contractors

Unveiling the Involvement of Private Companies, Academic Institutions, Judicial Bodies, and Security Organizations in Iran’s Internet Repression

Miaan Group | July 2023

About Us

The Miaan Group is a nonprofit organization, founded in 2019, providing legal and technical expertise, research, and advocacy support to organizations working on human rights. Miaan's Mission is to raise the capacity of civil society to promote human rights, good governance, and social justice through advocacy and technology.

CONTENTS

Executive Summary

This report investigates Internet control and surveillance in Iran, drawing on analysis of over 80,000 leaked emails pertaining to the Working Group for Determining Instances of Criminal Content (WGDICC) from 2014 to 2022. The WGDICC is a judicial body that operates under Iran's Attorney General's Office and filters and censors the Internet in Iran.

The emails were leaked in November 2022 by a group known as Anonymous Iran Ops and published on their Telegram channel. Additionally, this report relies on the information from Miaan Group's trusted sources at Iranian tech companies who spoke to us on condition of anonymity.

This report's findings come amid a context in which the Iranian government is pursuing a "national internet" project to tighten its grip on the online activities of its citizens. This project, known as the National Information Network (NIN), aims to create an online environment that favors local services and apps over international ones, by limiting their availability, speed, or affordability.

The NIN poses a serious threat to Iranians' Internet freedoms, as it grants the government more power over the internet infrastructure, online content, and users' personal data and online behaviors. However, the NIN relies on Iranian-developed services, from messaging apps to ride sharing apps, being hosted on servers inside the country. Importantly, sanctions have obliged this need by legally prohibiting Iranian developers from utilizing international Internet tools and platforms. In other words, they have left Iranians no choice but to use insecure domestic platforms and data infrastructure in line with the Iranian government's objectives.

Against this backdrop, the following are the main actors and entities that participate in the Iranian government's Internet control and suppression efforts. Below this, we present a list of recommendations from Miaan Group for how the US and EU governments, as well as multilateral institutions such as the UN, can best support Internet freedom in Iran:

» **Attorney General's Office:** This is a powerful judicial body that is responsible for prosecuting and punishing crimes, including those related to the Internet. It oversees the WGDICC, which filters and censors the Internet in Iran, and collaborates with various companies and technologies to develop surveillance and repression tools. The

Attorney General's Office also plays a role in shaping and implementing Iran's digital policy, and has been involved in international engagements on cybersecurity and Internet governance. The Attorney General's Office has been accused of violating human rights, suppressing dissent, and interfering in personal matters of dress and appearance.

» **Working Group for Determining Instances of Criminal Content (WGDICC):** The Internet in Iran is filtered and censored by this judicial body, which operates under the supervision of the Attorney General's Office. The WGDICC has an internal structure that consists of 12 members representing various bodies of the Islamic Republic, and is required to report its activities to the heads of three branches of the state and the Supreme National Security Council every six months. The WGDICC collaborates with various companies and technologies to develop surveillance and repression tools, such as Satra (Audiovisual Regulatory Authority), Yar Sharif Technologies Tuning Company, Niafam, Yaftar, and Douran Group.

» **The Supreme Council of Cyberspace (SCC):** A pivotal entity in Iran's digital landscape, playing a crucial role in the formulation and implementation of the country's Internet and digital policies. Established by Iran's Supreme Leader, the SCC functions as the highest-level policymaking body for cyberspace in Iran, tasked with managing, overseeing, and coordinating all cyber activities and strategies. Composed of various members from governmental, academic, and private sectors, it has the authority to regulate and supervise Iran's Internet infrastructure and activities. This includes areas such as information security, e-commerce, digital services, and cybercrime prevention, making the SCC a key player in shaping Iran's digital future.

» **Deputy Technical Deputy of Cyberspace Affairs of the Attorney General's Office:** The Deputy Technical Deputy of Cyberspace Affairs of the Attorney General's Office is a key figure in Iran's digital policy. This role is currently held by Javad Babaei (since April 26, 2020), whose previous position was as the Head of the Cybercrime Prosecution Office. Babaei coordinates the activities of various organizations and companies that work in this field. He also oversees the development of the Attorney General's Portal, a website that lets citizens report online crimes. However, the leaked emails reveal that he collaborates with the UN and travels abroad for this purpose, despite being involved in Internet suppression. For example, Mehdi Amiri, the Technical

Manager of his office, has played a prominent role in selecting Iranian representatives for the UN on cybersecurity and Internet governance issues, with the help of the "Cyberspace Developers Population (Pak)."

- **Satra (Audiovisual Regulatory Authority):** SATRA operates under the supervision of the IRIB, which is supervised by the Supreme Leader. This organization was established in 2016 in an attempt to monitor all online audio and video content published in Iran. In fact, this organization performs a similar role to the Ministry of Islamic Guidance in relation to online content. Satra has taken on numerous digital projects for the government, including the creation of an Internet blocking and censoring system for foreign websites and the development of the Attorney General's Portal. It was also revealed that Satra had a central role in the development of the "Smart Internet Blocking and Censoring" project.

- **Rasoul Jalili:** He is an appointed member of the SCC by the Supreme Leader and the president of Sharif University of Technology. In his roles, Jalili has played an instrumental role in shaping Iran's digital policy. He has spearheaded several initiatives including the conception of the Sharif Opening Plan. This controversial plan proposes a tiered Internet access system that would discriminate Internet access among individuals based on their professional and social statuses, thereby violating net neutrality principles and restricting information accessibility for a vast majority of Iranians. Furthermore, Jalili's involvement extends to the development of facial recognition and content Internet blocking and censoring tools for the WGDICC, demonstrating his significant influence over Iran's digital landscape. Through strategic promotion of companies carrying the "Sharif" name, Jalili has sought to foster a sense of trust and legitimacy among the public.

- **Yar Sharif Technologies Tuning Company:** This company was created by Rasoul Jalili with a primary purpose of assisting in the research and development of tools required by the Attorney General's Office, including the development of an "Electronic Evidence Documentation System." This company is involved in the creation of tools that can capture screenshots of chats, gather information on virtual accounts, and detect false information. The company also provides training programs for collecting evidence against detainees and developing third-party applications with capabilities to collect users' private information.

- **Iranian military forces:** The Iranian military forces, especially the Islamic Revolutionary Guards Corps (IRGC), are actively involved in formulating and proposing workflow solutions pertaining to the Internet, as well as implementing Internet censorship and surveillance measures. They also participate in training programs for collecting evidence against detainees and developing third-party applications with capabilities to collect users' private information. They have also attempted to militarize the Internet through measures such as the user protection parliamentary bill and increasing pressure on the SCC, but they have faced strong resistance from civil society activists who launched a campaign opposing the bill.

- **The Supreme National Defense University (SNDU):** This institution plays a major role in Iran's efforts toward Internet suppression and the militarization of cyberspace. Established by the Iranian Armed Forces, the SNDU is instrumental in the development and implementation of strategies pertaining to national security, including in the digital realm. The university contributes significantly to the formulation of Internet control tactics and tools, making it a cornerstone in Iran's infrastructure of Internet suppression.

- Additionally the WGDICC collaborates with various companies and technologies to develop surveillance and repression tools, such as:

- **Niafam:** This is a knowledge-based company that provides web-based solutions for organizations, such as intelligent portal systems, content management systems, online chat systems, customer relationship management systems, and online support systems. It also offers professional SEO services and custom software development. The leaked emails reveal Niafam's willingness to cooperate with the Attorney General's Office to launch an organizational portal with special capabilities. The proposed features include facial recognition and identification of individuals depicted in news images, aimed at enhancing the generated content.

- **Yaftar:** This is a company that has been working on an image analysis system since 2014 with the aim of identifying instances of "bad Hejab" and "nudity" in women's images. The company also has a long-term plan to develop web crawler systems to collect data from search engines such as Google, Yahoo, and Bing with the aim of proactive censorship.

» **Douran Group:** The Douran Group specializes in software and computer network services. It is a Internet blocking and censoring contractor named in the leaked emails. The company was sanctioned by the US Treasury Department for "censorship or other activities that limit freedom of expression or assembly." Douran has also established contracts with Internet providers to provide censorship equipment traffic analysis tools.

» **Gap Messenger:** This is a cross-platform encrypted cloud-based messenger that offers various features such as chat, group creation, channel creation, voice and video calls, wallet, bot platform, game and entertainment services, and online store creation. However, this messenger has engaged in censorship and provided user information to the Attorney General's Office. The CEO of Gap Messenger holds British citizenship and has established another company in England.

This report concludes that Iran's digital policy is driven by a strategic intent to control and regulate the Internet, which is evident in their efforts to develop sophisticated surveillance tools, initiate tiered Internet access, and implement legal VPN services. Iranian authorities also aim to increase control over Internet access and exert influence in international forums and the United Nations.

Recommendations for Tech Companies, U.S., UK, EU, and UN:

1. The US, UK, and EU should impose sanctions on the individuals and entities listed above for their role in Internet censorship and suppression in Iran, unless they have already been sanctioned.

    a. These include Rasoul Jalili and his companies, which are involved in developing censorship and surveillance tools. However, they should also avoid sanctioning academic institutions such as Sharif University, which are vital for connecting Iranians to the world and fostering innovation and education. Sanctions on these institutions could harm the Iranian people and society, rather than support them.

b. Overall, the US, UK, and EU should carefully assess the potential harm of any sanctions on Iranian-based or foreign technology and telecommunications companies or government entities. Sanctions can backfire and limit Iranians' access to a free and secure internet, rather than protect it. Therefore, US and European sanctions should steer clear of targeting "infrastructure level" technologies that are essential for the internet to function. Sanctions on these technologies could help the Iranian government isolate Iran's internet and control user behavior. Examples of infrastructure level technologies are internet gateways, internet service providers, mobile data providers, cloud services, and data centers.

2. All digital platforms, especially messaging and social media applications like WhatsApp, Telegram, Instagram, and Twitter, should consider incorporating features that enhance user privacy, such as an option to disable screenshots. While Signal has already implemented this feature, it should be more broadly adopted as a standard privacy measure across all similar platforms.

3. Technology companies should actively seek partnerships with civil society organizations and groups specializing in Internet freedom. These collaborations, particularly with those that possess a deep understanding of Iran's unique Internet policies and context, can help these companies continually refine their policies and services to better protect the security and privacy of Iranian users.

In particular, US- and EU-based technology companies should:

a. Enable access to their cloud infrastructures and support alternative payment channels like cryptocurrency, to provide secure services for Iranians inside the country. This would not only ensure the safety of Iranian users but also enable them to set up their own VPNs using international infrastructures.

b. Integrate proxies into their tools, especially secure communication applications like Wire or social media platforms such as Pleroma, and make them available free of charge to Iranian users. Proxies can help users bypass censorship and access blocked websites and services.

c. Develop and distribute guidelines and best practices for integrating proxies into communication tools, emphasizing the need for strong encryption, user-friendly interfaces, and minimal impact on performance and speed.

4. Policymakers in the EU and United States should similarly seek engagement with civil society and the Internet freedom community knowledgeable about Iran's Internet policies to ensure more informed, effective policy decisions. They should also urgently allocate funding to support VPNs and other circumvention technologies, which are essential for overcoming censorship and accessing information in Iran. In particular, they should:

   a. Invest in both scaling existing VPNs and circumvention technologies and developing new ones that use innovative architectures and techniques to resist censorship and blocking. Examples of such technologies include We-PN, which allows users outside Iran to share their internet connection with users inside the country; VPNs that use Iran-based servers to bypass mobile data shutdowns; DeltaChat, which uses Iran-based email networks to enable secure encrypted messaging during shutdowns of the international internet; and Snowflake, a VPN system that connects users to a massive network of decentralized servers.

   b. Invest in Starlink satellite dishes, which can provide a select number of users with relatively free internet access during periods of extreme disruption.

   c. Invest in technical research projects that collect and analyze data on Iran's National Information Network to gain more insight into its infrastructure, network connectivity issues, and censorship methods. This research would help VPN and tool developers to create technologies that work better in Iran.

   d. Invest in programming that increases the digital security of Iranians, such as public campaigns, accessible resources, help desks, and workshops and training sessions for activists, journalists, and civil society inside Iran. Changing user behaviors is a vital part of using the internet securely in Iran.

5. Google should investigate and take measures to prevent potential abuse of its services, such as the SafeSearch function, as tools for enforcing censorship by the Iranian government or other entities.

6. The UK and EU governments should enact and enforce policies that discourage and prevent its territory from being used as a safe haven for those involved in the development of tools for censorship and surveillance that infringe upon the rights of Iranians.

7. The United Nations should establish stricter policies and enforcement mechanisms to prevent those involved in the violation of Iranians' rights, particularly those developing censorship and surveillance tools, from influencing UN policies or gaining a voice within its various bodies.

8. Tech companies should comprehensively review and strengthen their policies related to third-party applications and APIs. They must ensure companies linked with the Iranian government do not have access or exploit these tools to infringe upon the rights of Iranians through censorship and surveillance measures.

9. Social media platforms, like Twitter, should strengthen their data policies to ensure their APIs and user data are not accessible to social media analysis companies associated with the Iranian government, thereby safeguarding user information and privacy.

Working Group to Determine Instances of Criminal Content

The Working Group for Determining Instances of Criminal Content (WGDICC), or the Internet Blocking and Censoring Committee, is a judicial body that enforces Article 22 of the Computer Crimes Law (2009), which requires it to vote on imposing filters on non-compliant websites every fifteen days at the Attorney General's Office. The WGDICC consists of 12 members representing various bodies of the Islamic Republic, and is required to report its activities to the heads of three branches of the state and the Supreme National Security Council every six months.

One of the emails. from 2019, examined reveals a letter titled "Important solutions and executive suggestions for organizing the virtual space" that is classified as "very confidential." It outlines the following solutions for regulating the Internet:

- Reducing bandwidth and gradually blocking foreign social media platforms, especially Instagram and WhatsApp, and disrupting or disabling effective audio and video communication, such as live streaming on these platforms.

- Completely blocking all unauthorized VPNs, circumvention tools, and Internet blocking and censoring evasion methods.

- Entrusting the Internet blocking and censoring system to access service providers and enabling them to provide legal monitoring capabilities directly to the judicial apparatus through the secretariat of the WGDICC.

The letter reveals the primary policy implemented under Ebrahim Raisi's tenure as Judiciary Chief, which aimed to reduce bandwidth and substitute unrestricted Internet access with tiered access levels. This also aligns with the statement of the current Minister of Information and Communications Technology on May 20, 2023, who said the country's foreign bandwidth needs are less than ten percent.

The letter also names Yaftar Pejohan Pishtaz Rayansh and Douran Data Processing as the main two contractors of online censorship in Iran, and states that they should work with the General Network Security Manager to counter Internet blocking and censoring circumvention tools, such as Psiphon. The letter also suggests that if the Ministry of Communications fails to block these tools, this responsibility should be transferred to the IRGC by issuing a judicial order. The letter also requests that blocking technology be transferred to Internet providers.

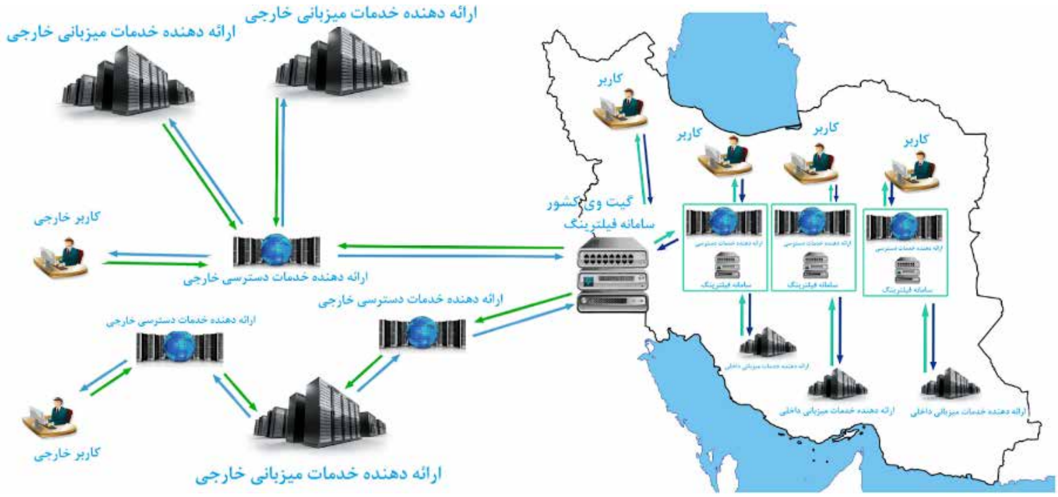
According to Miaan Group's trusted sources at Iranian tech companies, different operators have different Internet blocking and censoring methods and policies, depending on their contracts with Internet blocking and censoring companies. However, these companies do not necessarily follow the instructions of their employers, because Internet blocking and censoring affects their traffic consumption and income. For example, Douran provides Internet blocking and censoring tools and services to Mebinnet, Irancell, HiWeb, ParsOnline and Asiatech. Hamrah Aval (MCI) works with Yaftar and TCI also cooperates with Douran. The ITC itself also receives these services from Douran. Sahab Pardaz operates at a higher level compared to Douran and Yaftar, and is responsible for reviewing and announcing policies and technical architecture. Please note that the documents providing evidence for these assertions are available upon request.

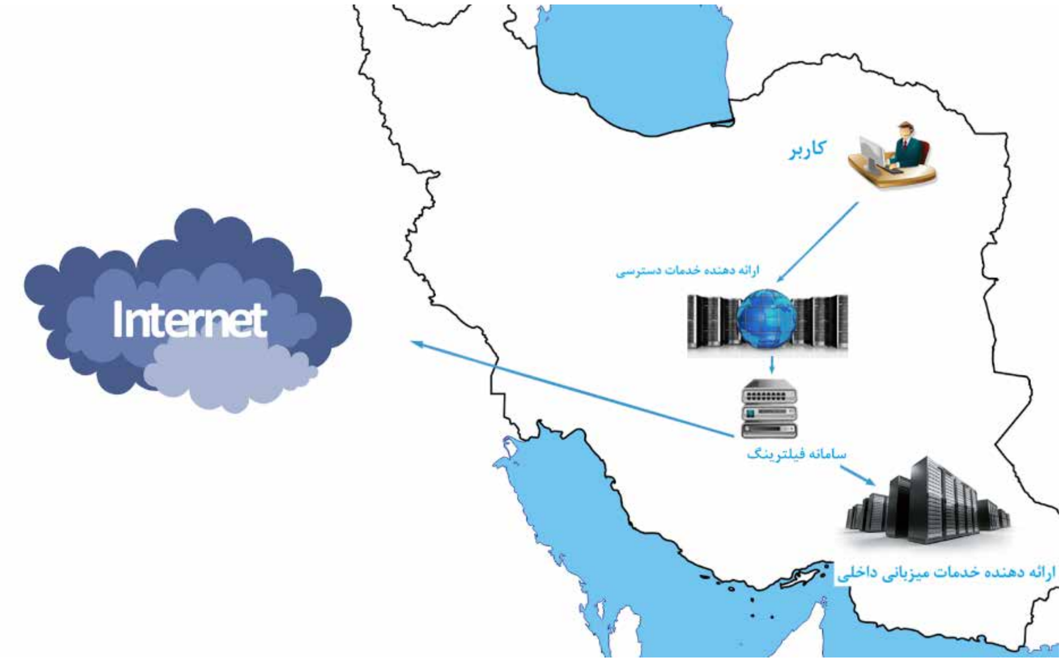
Furthermore, the letter refers to the "proposed workflow solutions of the General Staff of the Armed Forces to the Supreme Leader." This indicates that the Iranian military forces are actively involved in formulating and proposing workflow solutions pertaining to the Internet. It suggests an attempt to gain control over the Internet and potentially militarize its operations, further highlighting the influence and aspiration of the military in shaping Internet governance and control in Iran.

The Two Levels of Internet Censorship in Iran

The emails confirm what we have long surmised is the design of Iran's Internet infrastructure, namely that it consists of two levels of censorship: the country's gateway and the Internet service providers (ISPs). The country's gateway is a centralized entry point that controls Internet traffic flow in and out of the country, managed by the infrastructure telecommunications company. Within the country, there is also an internal network, or intranet, known as the National Information Network (NIN).

These maps confirm and illustrate the previous analysis and research on the Internet structure in Iran:


ارائه دهنده خدمات میزبانی خارجی
ارائه دهنده خدمات میزبانی خارجی
کاربر خارجی
ارائه دهنده خدمات دسترسی خارجی
ارائه دهنده خدمات دسترسی خارجی
ارائه دهنده خدمات دسترسی خارجی
کاربر خارجی
ارائه دهنده خدمات میزبانی خارجی
کاربر
کاربر
کاربر
کاربر
گیت وی کشور
سامانه فیلترینگ
ارائه دهنده خدمات دسترسی
سامانه فیلترینگ
ارائه دهنده خدمات دسترسی
سامانه فیلترینگ
ارائه دهنده خدمات دسترسی
سامانه فیلترینگ
ارائه دهنده خدمات میزبانی داخلی
ارائه دهنده خدمات میزبانی داخلی
ارائه دهنده خدمات میزبانی داخلی



The Roles and Responsibilities of the WGDICC Staff

In December 2020, the emails and an accompanying Excel file reveal the names, positions, and projects of the WGDICC's primary employees, who work on various aspects of Internet blocking and censoring. The most influential and authoritative individuals among them are Mehdi Amiri, the Deputy Technical Supervisor for Cyber Affairs at the Attorney General's Office; Abbaszadeh, the Deputy Director of the National Information Network Resources Management Office; and Javad Babaei, the Deputy for Cyber Affairs at the Judiciary.

The table below shows the schedule and work shifts of the WGDICC employees, along with their positions and assigned projects:

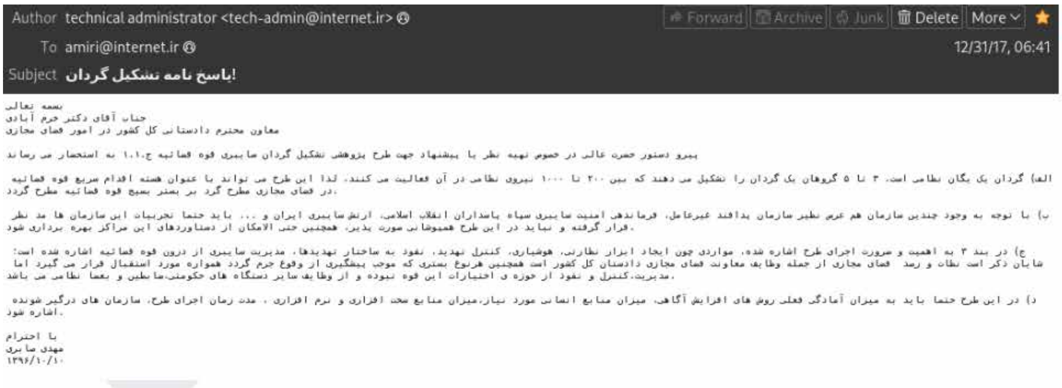
Name	Position/Description
Doyesti	Preprocessing
Doyesti	Host Extraction and Domain Information Robot
Shabannia	Designing Executive Unit's UI
Mehdi Saberi	Important Sites Systems
Mehdi Saberi	Protest Sites (RAVA)

Abdollahi	Order Registration Panel
Nasaji	Logging All Statuses
Nasaji	Registration Identified Hosts
Nasaji	Sending Links to Fix Unit
Nasaji	Identifying Hosts of Criminal Sites
Nasaji	Documenting Fix Effect
Ahmadi	Sending Notices & Comments to
Ahmadi	Observer
	Sending Identification Notices to Host
Ahmadi	Warning Monitoring Unit (Blocking)
Ahmadi	Warning Monitoring Unit (Internet
Ahmadi	blocking and censoring)
	Sending Notice to Inspection Unit
Ahmadi	TDL and SLD Investigations
Ahmadi	Intelligent url Blocking Detection
Abdollahi / Mehdi Saberi	Sending Batch Reminder Commands
Abdollahi / Medi Saberi	Cleansings and Decleansings in
	Batches
Abdollahi / Mehdi Saberi	Blockings in Batches
Abdollahi / Mehdi Saberi	Sending User-Oriented Commands in
Abdollahi / Mehdi Saberi	Batches
	Domain Blocking in Batches
Abdollahi / Mehdi Saberi	Sending Complaints to RAVA
Mehdi Saberi / Nasaji	Database Design and Development
Doyesti	(continuous process)
	Site Managers Conversion and
Doyesti	Transfer to New Organization
	Host Managers Conversion and
Doyesti / Abdollahi	Transfer to New Organization
	NS Users Conversion in New Systems
Nasaji	With Existing Hosting
	Reviewing All Written Codes

The Cyber Battalion of the Judiciary

An email from Mehdi Saberi, the technical director of the Attorney General's Office, to Mehdi Amiri reveals a plan to form a Cyber Battalion of the judiciary, following an order from Khorramabadi, the then Deputy Attorney General of the country for Cyberspace Affairs.

The plan, called the "Judiciary Rapid Response in Cyberspace," designates the Basij of the judiciary as the operative force for this battalion. The email also mentions the existence of several other organizations with similar tasks, such as the Passive Defense Organization, the Cyber Security Command of the Islamic Revolutionary Guard Corps (IRGC), and the Cyber Army of Iran.



Author technical administrator <tech-admin@internet.ir>
To amiri@internet.ir
12/31/17, 06:41
Subject پاسخ نامه تشکیل گردان!

بسمه تعالی
جناب آقای دکتر خرم آبادی
معاون محترم دادستانی کل کشور در امور فضای مجازی

پیرو دستور حضرت عالی در خصوص تهیه نظر یا پیشنهاد جهت طرح پژوهشی تشکیل گردان سایبری قوه قضائیه ج.۱.۱ به استحضار می رساند

الف) گردان یک یگان نظامی است. ۳ تا ۵ گروهان یک گردان را تشکیل می دهند که بین ۳۰۰ تا ۱۰۰۰ نیروی نظامی در آن فعالیت می کنند. لذا این طرح می تواند با عنوان هسته اقدام سریع قوه قضائیه
در فضای مجازی مطرح گرد بر بستر بسیج قوه قضائیه مطرح گردد.

ب) با توجه به وجود چندین سازمان هم عرض نظیر سازمان پدافند غیرعامل، فرماندهی امنیت سایبری سپاه پاسداران انقلاب اسلامی، ارتش سایبری ایران و ... باید حتما تجربیات این سازمان ها مد نظر
قرار گرفته و نباید در این طرح همپوشانی صورت پذیرد. همچنین حتی الامکان از دستاوردهای این مراکز بهره برداری شود.

ج) در بند ۳ به اهمیت و ضرورت اجرای طرح اشاره شده. مواردی چون ایجاد ابزار نظارتی، هوشیاری، کنترل تهدید، نفوذ به ساختار تهدیدها، مدیریت سایبری از درون قوه قضائیه اشاره شده است:
شایان ذکر است نظارت و رصد فضای مجازی از جمله وظایف معاونت فضای مجازی دادستان کل کشور است همچنین هرنوع بستری که موجب پیشگیری از وقوع جرم گردد همواره مورد استقبال قرار می گیرد اما
مدیریت،کنترل و نفوذ از حوزه ی اختیارات این قوه نبوده و از وظایف سایر دستگاه های حکومتی،امنیتی و بعضا نظامی می باشد.

د) در این طرح حتما باید به میزان آمادگی فعلی روش های افزایش آگاهی، میزان منابع انسانی مورد نیاز،میزان منابع سخت افزاری و نرم افزاری ، مدت زمان اجرای طرح، سازمان های درگیر شونده
اشاره شود.

با احترام
مهدی صابری
۱۳۹۶/۱۰/۱۰

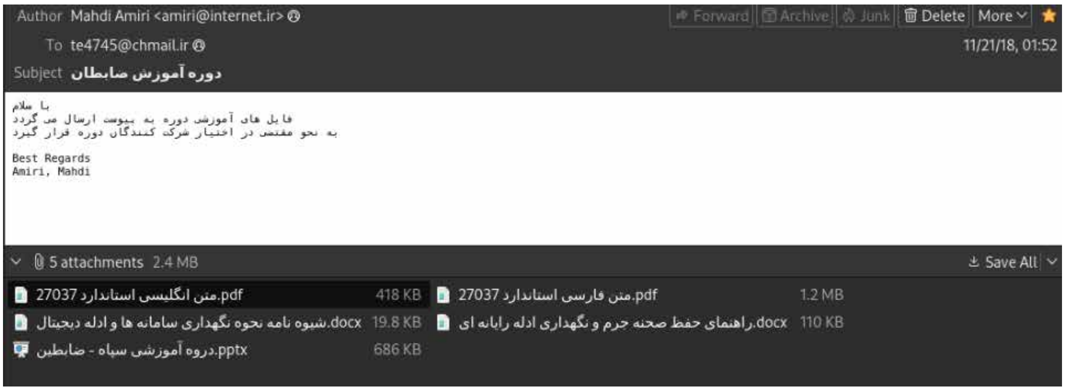
While this letter confirms the existence of the cyber army, it does not delve into its specific details. However, in paragraph b, it mentions the utilization of the cyber army in the following manner:

"b) Considering the existence of several organizations with the same tasks, such as the Passive Defense Organization, the Cyber Security Command of the Islamic Revolutionary Guard Corps, the Cyber Army of Iran, and etc the experiences of these organizations must be used."

Training Sessions for IRGC Officers

In November 2018 the Attorney General's Office organized training sessions for individuals referred to as "judicial officers," as shown by an email to te4745@chmail.ir with five attachments, including a PowerPoint file named "IRGC training course." This file contains the training material developed specifically for IRGC officers, with the goal of "protecting the crime scene and basic measures to protect crime evidence."

The training sessions for IRGC officers are significant because they indicate a change in the arrest procedures. In the past, the documents and evidence of the suspects were not examined quickly, but now they are collected and labeled as "crime documents". This has led to faster screening and arrest of the activists, which is the outcome of this training.



Author Mahdi Amiri <amiri@internet.ir>
To te4745@chmail.ir
11/21/18, 01:52
Subject دوره آموزش ضابطان

```
با سلام
فایل های آموزش دوره به پیوست ارسال می گردد
به نحو مقتضی در اختیار شرکت کنندگان دوره قرار گیرد

Best Regards
Amiri, Mahdi
```

5 attachments 2.4 MB

متن انگلیسی استاندارد 27037.pdf	418 KB	متن فارسی استاندارد 27037.pdf	1.2 MB
شیوه نامه نحوه نگهداری سامانه ها و ادله دیجیتال.docx	19.8 KB	راهنمای حفظ صحنه جرم و نگهداری ادله رایانه ای.docx	110 KB
دروه آموزشی سپاه - ضابطین.pptx	686 KB		

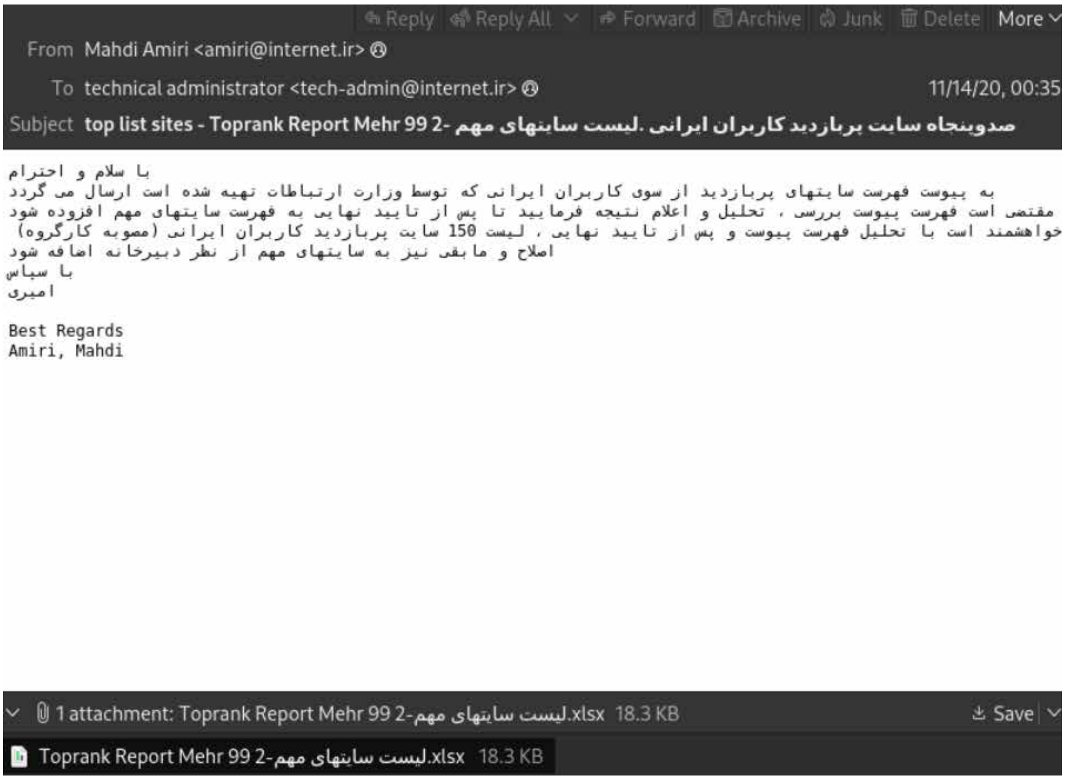
Internet Pricing

The Attorney General's Office emails reveal that they have a say in determining the pricing of domestic websites, which is a key component of the NIN project. The NIN aims to create an online environment that favors local services and apps over international ones, by making them cheaper, faster, or more available. One of the ways to achieve this is by offering half-price domestic websites, which are websites that are hosted on servers inside Iran and registered in the system of the Information Technology Organization of Iran.

An email from Mehdi Amiri to the technical department of the Attorney General's Office includes a list of popular websites prepared by the Ministry of Communications and Information Technology through an analysis of Iranian users' traffic.

The list has been officially published on the website of the Information Technology Organization of Iran, under the title "List of Domestically Hosted Internet Domains Registered in the System." The email suggests that the Attorney General's Office has the authority to confirm this list, challenging previous assumptions that attributed such decisions to the Ministry of Communications or the Supreme Cyberspace Council.

Another email from Yaftar's project manager in November 2015, explains



From Mahdi Amiri <amiri@internet.ir>
To technical administrator <tech-admin@internet.ir> 11/14/20, 00:35
Subject top list sites - Toprank Report Mehr 99 2- لیست سایتهای مهم .صدوپنجاه سایت پربازدید کاربران ایرانی

```
با سلام و احترام
به پیوست فهرست سایتهای پربازدید از سوی کاربران ایرانی که توسط وزارت ارتباطات تهیه شده است ارسال می گردد
مقتضی است فهرست پیوست بررسی ، تحلیل و اعلام نتیجه فرمایید تا پس از تایید نهایی به فهرست سایتهای مهم افزوده شود
خواهشمند است با تحلیل فهرست پیوست و پس از تایید نهایی ، لیست 150 سایت پربازدید کاربران ایرانی (مصوبه کارگروه)
اصلاح و مابقی نیز به سایتهای مهم از نظر دبیرخانه اضافه شود
با سپاس
امیری

Best Regards
Amiri, Mahdi
```

1 attachment: Toprank Report Mehr 99 2-لیست سایتهای مهم.xlsx 18.3 KB Save

Toprank Report Mehr 99 2-لیست سایتهای مهم.xlsx 18.3 KB

how SafeSearch functionality can remove "immoral content" from search results in search engines like Google, Yahoo, and Bing. He states that if the SafeSearch feature is disabled by the user in the Yahoo search engine, the Internet blocking and censoring system will activate it and prevent immoral content from being displayed to the user.

This email exchange, which occurred on November 17, 2015, focused on utilizing Google as a means to uncover "criminal" content. Within this context, the employment of SafeSearch as a tool for censorship was brought up. Importantly, SafeSearch, originally designed as a feature to block inappropriate content, was discussed in relation to controlling access to certain types of information. Ultimately, on July 12, 2022, the Telecommunication Infrastructure Company began interfering and hijacking DNSs (Domain Name System) to redirect users inside Iran who wanted to visit Google's search engine to Google SafeSearch as a means of suppressing and censoring Internet content.

Collecting Information on IP Addresses Ranges

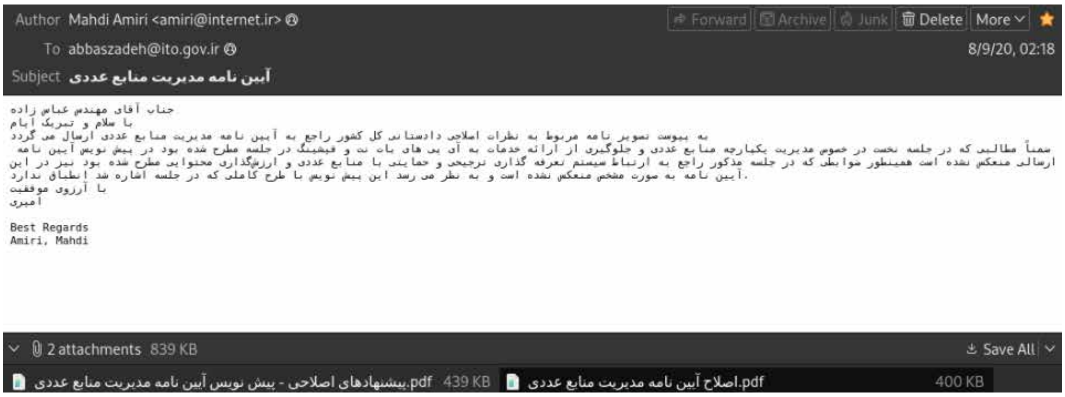
The emails reveal that Mehdi Amiri, the technical director, and engineer Abbaszadeh, the Deputy General Directorate of Resource Management of the National Information Network, exchanged 531 emails between September

14, 2020, and October 14, 2021. These emails requested information on the IP owners of certain companies that were allegedly involved in "criminal acts."

This email exchange between Mehdi Amiri and engineer Abbaszadeh raises questions about the legitimacy and transparency of the IP information requests. There is no clear procedure for obtaining and sharing this information with the National Information Network. The IP owners are not informed or consulted about these requests. This suggests that the Network has the ability to spy on or censor the activities of certain companies that are accused of "criminal acts."

IP Regulations

The emails also reveal an IP addresses regulation that bans the use of non-Iranian IP addresses for bypassing censorship through tunneling methods. In other words, this exposes for the first time that authorities are criminalizing the use of foreign IP addresses to access blocked websites through tunneling methods. The regulation says, "According to Article 3 of the instructions for organizing access and with regards to the needs of individuals and specialized groups in cyberspace, any tunnel and VPN to abroad requires permission from the Working Group to Determine Instances of Criminal Content."



Author Mahdi Amiri <amiri@internet.ir>
To abbaszadeh@ito.gov.ir
8/9/20, 02:18
Subject آیین نامه مدیریت منابع عددی

جناب آقای مهندس عباس زاده
با سلام و تبریک ایام
به پیوست تصویر نامه مربوط به نظرات اصلاحی دادستانی کل کشور راجع به آیین نامه مدیریت منابع عددی ارسال می گردد
ضمناً مطالبی که در جلسه نخست در خصوص مدیریت یکپارچه منابع عددی و جلوگیری از ارائه خدمات به آی پی های بات نت و فیشینگ در جلسه مطرح شده بود در پیش نویس آیین نامه
ارسالی منعکس نشده است همینطور ضوابطی که در جلسه مذکور راجع به ارتباط سیستم تعرفه گذاری ترجیحی و حمایتی با منابع عددی و ارزشگذاری محتوایی مطرح شده بود نیز در این
آیین نامه به صورت مشخص منعکس نشده است و به نظر می رسد این پیش نویس با طرح کاملی که در جلسه اشاره شد انطباق ندارد.
با آرزوی موفقیت
امیری

Best Regards
Amiri, Mahdi

2 attachments 839 KB
Save All
پیشنهادهای اصلاحی - پیش نویس آیین نامه مدیریت منابع عددی.pdf 439 KB
اصلاح آیین نامه مدیریت منابع عددی.pdf 400 KB

The regulation was introduced on September 8, 2020 and indicates a significant development in the establishment of a tiered Internet access system. According to this regulation, the use of the 8/10 private IP address range should only be used for the development of the national information network. By reserving this IP address range for internal use, it suggests a segregated network that operates separately from the global Internet.

Censorship Requests and Information Gathering

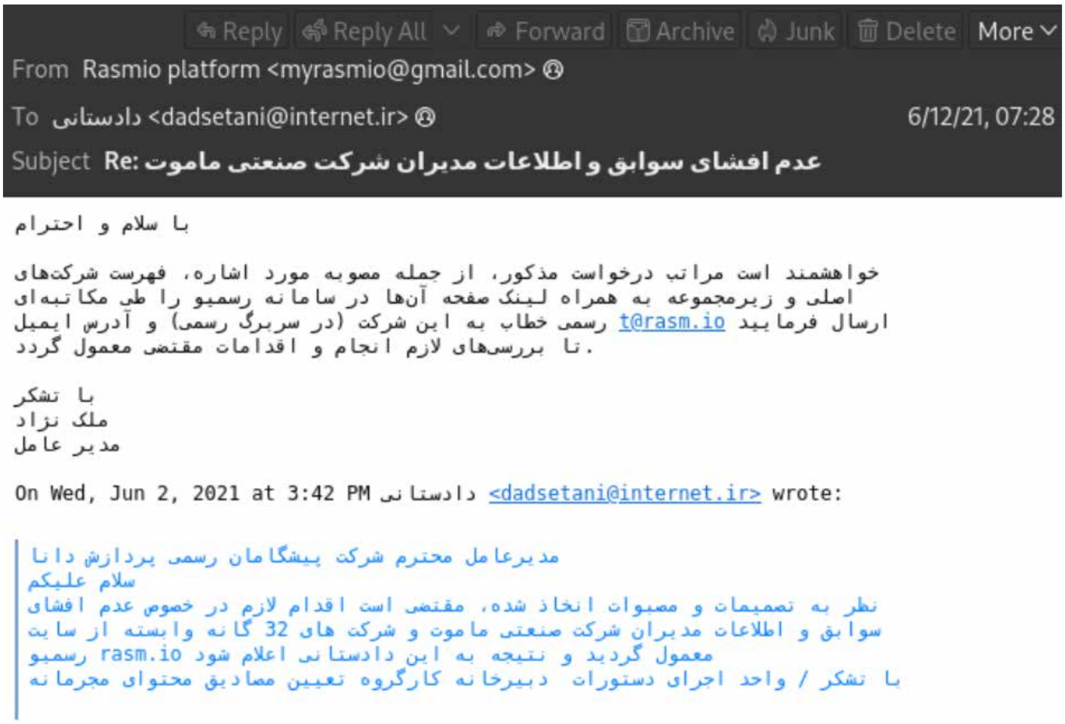
IRGC Organized Crime Investigation Center

The emails show that the WGDICC receives and sends requests for censorship and blocking from and to various entities, such as the IRGC Organized Crime Investigation Center (Gardab), Rasimo, and Kashef Secure Electronic Processing. These requests cover different types of online content, such as Telegram channels, Instagram tags, information related to specific companies and individuals, gambling, and financial transactions.

Gardab is the most active entity in requesting censorship and blocking, especially for Telegram channels like Amad news and other online content. Gardab is also responsible for online repression and arresting and imprisoning Iranian citizens for their online activity. Many activists and civil society members have been arrested by Gardab in recent years based on their online expressions.

Content Moderation

Internet blocking and censoring are not limited to specific websites or social media platforms. For example, emails exchanged between the Working Group for Determining Instances of Criminal Content and Rasimo, a platform for communication and business analysis, shows that the Attorney



From Rasmio platform <myrasmio@gmail.com>

To دادستانی <dadsetani@internet.ir>

6/12/21, 07:28

Subject Re: عدم افشای سوابق و اطلاعات مدیران شرکت صنعتی ماموت

با سلام و احترام

خواهشمند است مراتب درخواست مذکور، از جمله مصوبه مورد اشاره، فهرست شرکت‌های
اصلی و زیرمجموعه به همراه لینک صفحه آن‌ها در سامانه رسمیو را طی مکاتبه‌ای
رسمی خطاب به این شرکت (در سربرگ رسمی) و آدرس ایمیل t@rasm.io ارسال فرمایید
تا بررسی‌های لازم و انجام اقدامات مقتضی معمول گردد.

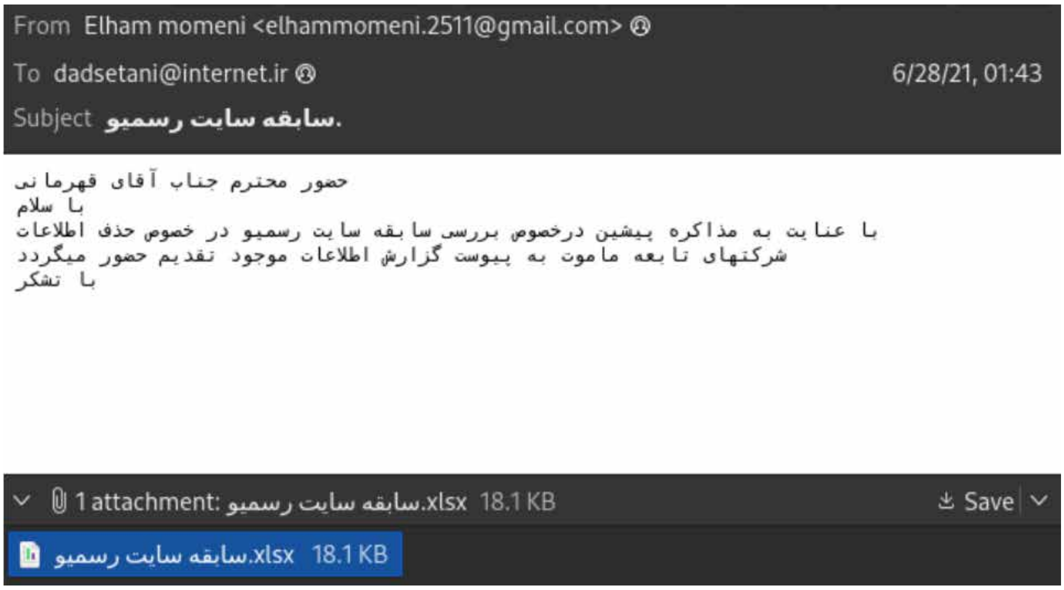
با تشکر
ملک نژاد
مدیر عامل

On Wed, Jun 2, 2021 at 3:42 PM دادستانی <dadsetani@internet.ir> wrote:

> مدیرعامل محترم شرکت پیشگامان رسمی پردازش دانا
> سلام علیکم
> نظر به تصمیمات و مصبوات اتخاذ شده، مقتضی است اقدام لازم در خصوص عدم افشای
> سوابق و اطلاعات مدیران شرکت صنعتی ماموت و شرکت های 32 گانه وابسته از سایت
> رسمیو rasm.io معمول گردید و نتیجه به این دادستانی اعلام شود
> با تشکر / واحد اجرای دستورات دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه

General's Office has requested the removal of certain information related to specific companies and individuals from this platform.

The Attorney General's Office has requested the removal of various individuals and companies from the Rasimo platform. Among the individuals mentioned are Behrouz Ferdows, Behzad Ferdows, Mehrzad Ferdows, and Mitra Ferdows. Additionally, several companies, including Mammut Industrial Group, Hag Bar transport company, Mayan Automotive Group, Mehrsa construction prefabrication company, Karamad Leasing company, Mammut steel structures, Mammut Teleca, Raman Automotive, Mammut Diesel, Nikan Mammut Charity Organization, Mammut Group, Atin Part Afzar, and several others, were also listed for removal.



From Elham momeni <elhammomeni.2511@gmail.com>
To dadsetani@internet.ir 6/28/21, 01:43
Subject .سابقه سایت رسمیو

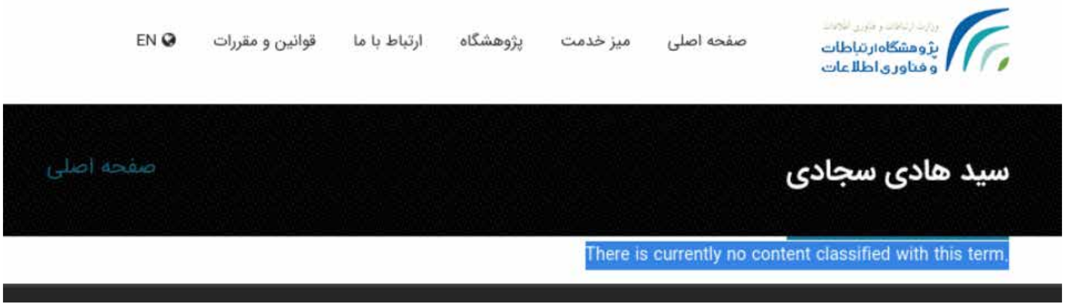
حضور محترم جناب آقای قهرمانی
با سلام
با عنایت به مذاکره پیشین درخصوص بررسی سابقه سایت رسمیو در خصوص حذف اطلاعات
شرکتهای تابعه ماموت به پیوست گزارش اطلاعات موجود تقدیم حضور میگردد
با تشکر

1 attachment: سابقه سایت رسمیو.xlsx 18.1 KB
سابقه سایت رسمیو.xlsx 18.1 KB

The emails related to the removal of individuals and companies from the Rasimo platform do not specify the reasons behind these requests. However, this example highlights that the Working Group for Determining Instances of Criminal Content operates with a broader scope than solely deciding to block websites or apps. It indicates that they also monitor and exercise authority over the content within domestic services.

Information Communication Research Institute

The emails show that Seyyed Hadi Sajjadi plays a significant role in the design and research of national information network development programs. He is the head of the Information Communication Research Institute, formerly known as the Telecommunication Research Center. After the disclosure of these emails, his personal information was removed from public access on the Institute's website, suggesting a response to the exposure of sensitive information and a desire to limit public visibility or access to personal details.

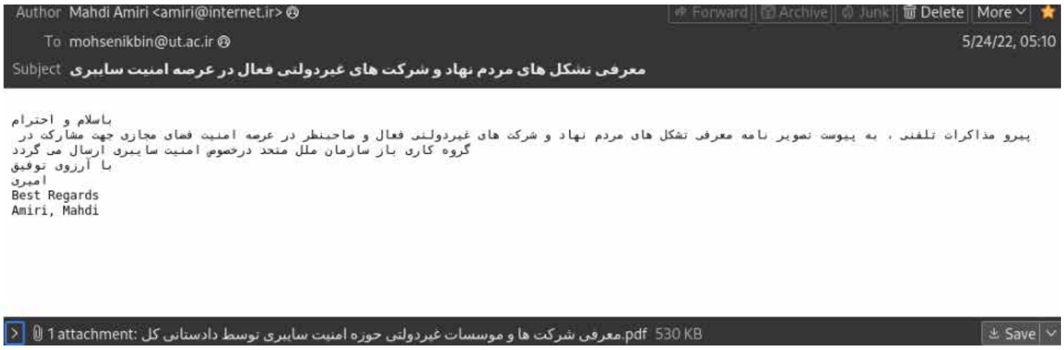

وزارت ارتباطات و فناوری اطلاعات
پژوهشگاه ارتباطات و فناوری اطلاعات
صفحه اصلی
میز خدمت
پژوهشگاه
ارتباط با ما
قوانین و مقررات
EN
صفحه اصلی

سید هادی سجادی

There is currently no content classified with this term.

Governmental NGOs (GONGOs)

The emails reveal that the Attorney General's Office supports certain organizations that are registered as non-governmental but seemingly act in favor of the government. For example, Mehdi Amiri, the technical manager of the Attorney General's Office, corresponded with Mohsen Nikban from Tehran University and shared a list of companies that are active in the field of cybersecurity. These companies have been identified as potential participants in "the meetings of the open working group on international information and communication security" at the UN.



Author Mahdi Amiri <amiri@internet.ir>
To mohsenikbin@ut.ac.ir
5/24/22, 05:10
Subject معرفی تشکل های مردم نهاد و شرکت های غیردولتی فعال در عرصه امنیت سایبری

```
باسلام و احترام
پیرو مذاکرات تلفنی ، به پیوست تصویر نامه معرفی تشکل های مردم نهاد و شرکت های غیردولتی فعال و صاحبنظر در عرصه امنیت فضای مجازی جهت مشارکت در
گروه کاری باز سازمان ملل متحد درخصوص امنیت سایبری ارسال می گردد
با آرزوی توفیق
امیری
Best Regards
Amiri, Mahdi
```

1 attachment: معرفی شرکت ها و موسسات غیردولتی حوزه امنیت سایبری توسط دادستانی کل.pdf 530 KB

Attached to the letter dated May 24, 2022, the Vice-President of Cyberspace Affairs of the Attorney General's Office has sent a letter to Eshraq Jahani, Director General of International Peace and Security at the Ministry of Foreign Affairs. The letter includes a list of the following companies:

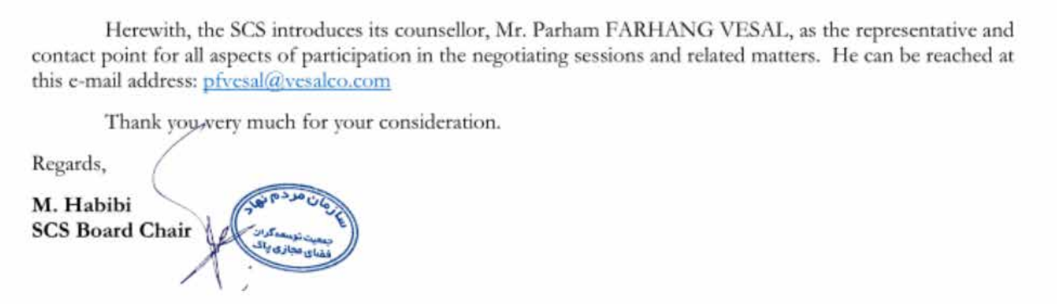
- Amnpardaz Soft Corporation
- Raya Security Research Institute of Sharif Systems affiliated to Sharif

University

- Amn Afzar Gostaresh Sharif affiliated with Sharif University
- Mahiman Information and Communication Technology Group
- Faraz Pejohan
- Research Center of Information Industries
- Amn Naji Development technology laboratory
- Simorgh Instrument Monitoring Company

Clean Cyberspace Developers Association

The Clean Cyberspace Developers Association (CCDA) is a Government-Organized Non-Governmental Organization (GONGO) mentioned in the emails. FilterWatch previously mentioned CCDA in its profile of Eisa Zarepour, the current Minister of Information and Communications Technology, who was a founding member and an alternate board member of CCDA in 2016. The association was founded by a group of hardline policymakers and asserts that its activities are mainly focused on Internet policy in Iran that support "the values and ideals of the Islamic Revolution." CCDA advocates for extensive web Internet blocking and censoring measures and perceives social media applications as a threat to Iran's national sovereignty.



Herewith, the SCS introduces its counsellor, Mr. Parham FARHANG VESAL, as the representative and contact point for all aspects of participation in the negotiating sessions and related matters. He can be reached at this e-mail address: pfvesal@vesalco.com

Thank you very much for your consideration.

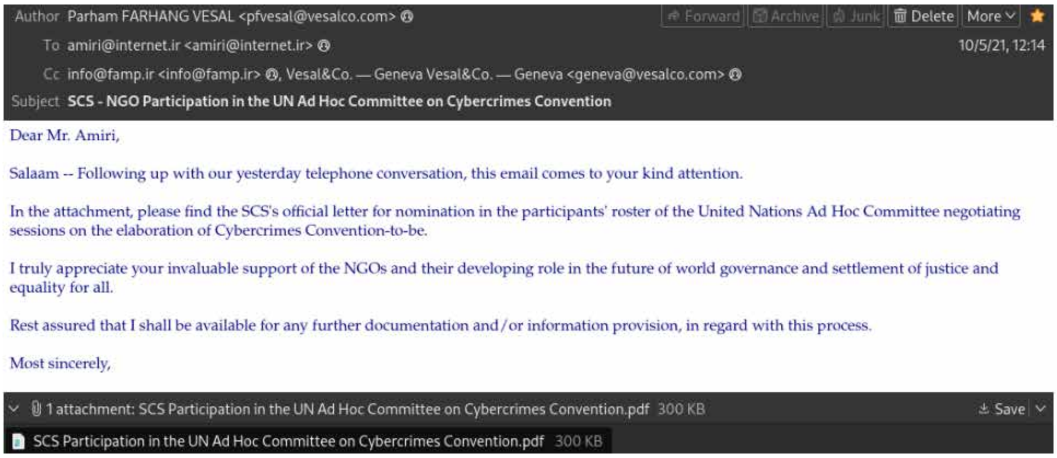
Regards,

M. Habibi
SCS Board Chair

سازمان مردم نهاد
جمعیت توسعه‌گران
فضای مجازی پاک

Several founding members of CCDA are directly connected to Iran's Supreme Leader Khamenei, including its managing director, Rasool Jalili, who was appointed by the Supreme Leader to the Supreme Council of Cyberspace, and Monira Hosseini-Khamenei, who serves as the board's vice chairman and is a relative of Ayatollah Khamenei.

According to an email from Parham Farhang Vesal, he was appointed as CCDA's counselor and informed the Attorney General's Office that CCDA had been nominated for inclusion in the participants roster of the UN Ad Hoc committee negotiating sessions on the elaboration of a cybercrimes convention.



Author Parham FARHANG VESAL <pfvesal@vesalco.com>
To amiri@internet.ir <amiri@internet.ir>
10/5/21, 12:14
Cc info@famp.ir <info@famp.ir>, Vesal&Co. — Geneva Vesal&Co. — Geneva <geneva@vesalco.com>
Subject SCS - NGO Participation in the UN Ad Hoc Committee on Cybercrimes Convention

Dear Mr. Amiri,

Salaam -- Following up with our yesterday telephone conversation, this email comes to your kind attention.

In the attachment, please find the SCS's official letter for nomination in the participants' roster of the United Nations Ad Hoc Committee negotiating sessions on the elaboration of Cybercrimes Convention-to-be.

I truly appreciate your invaluable support of the NGOs and their developing role in the future of world governance and settlement of justice and equality for all.

Rest assured that I shall be available for any further documentation and/or information provision, in regard with this process.

Most sincerely,

1 attachment: SCS Participation in the UN Ad Hoc Committee on Cybercrimes Convention.pdf 300 KB

SCS Participation in the UN Ad Hoc Committee on Cybercrimes Convention.pdf 300 KB

Contractors of Censorship and Suppression

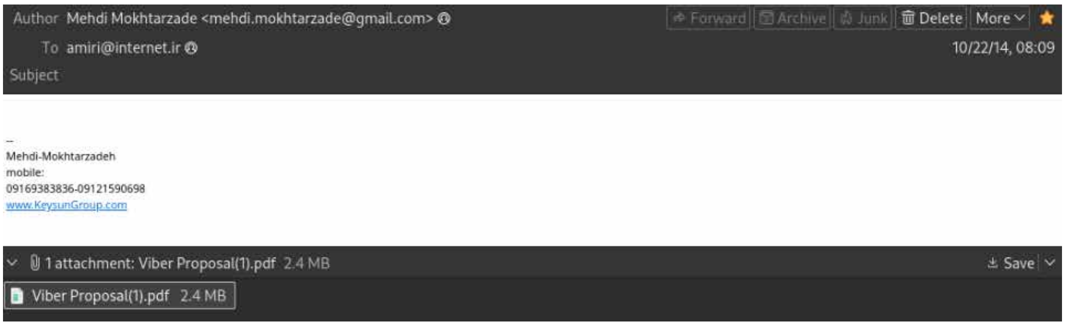
The emails reveal the contractors that have worked with the Attorney General's Office from 2014 until the time of the anonymous hackers' leak. We only focus on the companies that developed tools for repression and censorship. For example, we exclude Tebian, which hosts Internet.ir, the website of the Attorney General's Office, because it is not relevant to our report.

Sahab Pardaz

Sahab Pardaz, officially known as Samaneh Gostar Sahab Pardaz, is one of the key players in blocking and censoring operations, stating on its website that it provides solutions in data strategy and technology to various organizations. Established in 2013, the company claims to have 180 employees specialized in data science, macrodata, and distributed systems. The company was sanctioned by the US Treasury Department in October 2022 "as one of the main operators of social media Internet blocking and censoring services in Iran." In response, the company acknowledged that the Iranian government is one of its customers but denied that its products have limited Iranians' access to the Internet.

Keysun Data Processing

On October 22, 2014, Keysun sent a proposal to the Attorney General's Office titled "Viber software security analysis project." Viber was a very popular messenger in Iran that lost its users due to extensive disruptions by the Iranian authorities, but it is still used by some users in Iran. This company proposed the use of spamming techniques on Viber and requested a budget of 64 million Tomans for its implementation.



Author Mehdi Mokhtarzade <mehdi.mokhtarzade@gmail.com>
To amiri@internet.ir
10/22/14, 08:09
Subject

--
Mehdi-Mokhtarzadeh
mobile:
09169383836-09121590698
www.KeysunGroup.com

1 attachment: Viber Proposal(1).pdf 2.4 MB
Viber Proposal(1).pdf 2.4 MB

Based on this proposal, they were supposed to collect phone numbers of Iranian Viber users during this project.

The company stated the following advantages of this project:

- Finding a list of Viber users in Iran, including their phone numbers and photos.
- Engaging in psychological warfare by using the information obtained from the first advantage.
- Demonstrating strength in the field of information technology by publishing a report that highlights weaknesses or vulnerabilities within the Viber program.
- Creating fear by using programs that send Viber codes or phones to target Viber users or non-users.
- Creating a group within Viber and extracting or disseminating information from or to group members.
- Sending automatic text, video, location, and audio messages individually or within a group on Viber.
- Conducting surveys and researching the behavior of Viber users, potentially using an international template project, and then dumping the information.
- Announcing vulnerabilities or weaknesses of Viber to internal users to enhance their understanding and usage.
- Creating honey pots by activating 122 individuals with specific photos and characteristics as bait within Viber.
- Sending a malicious message, which is suggested to be combined with other methods.

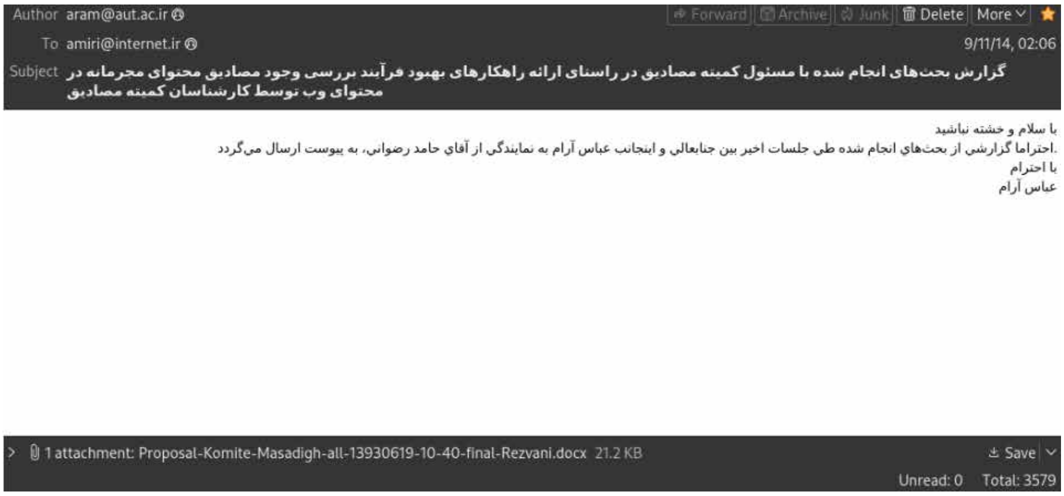
Of note, General Seyed Kamal Hadianfar, head of FATA police at the time, said in an interview with Khabar Online on September 21, 2014, “You should know that private messages on Viber, WhatsApp, etc. can be controlled by FATA police.”

Yaftar Pajouhan Pishtaz Rayanesh Company

The emails indicate that the Yaftar company is involved in website and app Internet blocking and censoring, as well as image analysis and facial recognition, in collaboration with the judiciary. Yaftar Pezohan Pishtaz Rayansh company was established on April 19, 2013. Mustafa Rezvani (saved version) is the current CEO of this company. He was previously the manager of "Amanfazar Gostar Sharif " company.

Contract no 4119; Traffic Analysis and Internet Censorship

An email from Abbas Aram on November 19, 2014, included an attachment that contained discussions regarding the agreement between Yaftar Company and Mohammad Javad Azari Jahormi, who was the head of ITC at that time. The letter, sent by Abbas Aram on behalf of Mustafa Rizvani, the manager of Yaftar Company, was addressed to Azari Jahormi. It appears that this email was sent to the Attorney General's Office by mistake, because a few seconds later, another email was sent asking them not to read the previous email and to delete it.



Author aram@aut.ac.ir
To amiri@internet.ir
9/11/14, 02:06
Subject گزارش بحث‌های انجام شده با مسئول کمیته مصادیق در راستای ارائه راهکارهای بهبود فرآیند بررسی وجود مصادیق محتوای مجرمانه در محتوای وب توسط کارشناسان کمیته مصادیق

با سلام و خشته نباشید
احتراما گزارشي از بحث‌هاي انجام شده طي جلسات اخير بين جنابعالي و اينجانب عباس آرام به نمايندگي از آقاي حامد رضواني، به پيوست ارسال مي‌گردد.
با احترام
عباس آرام

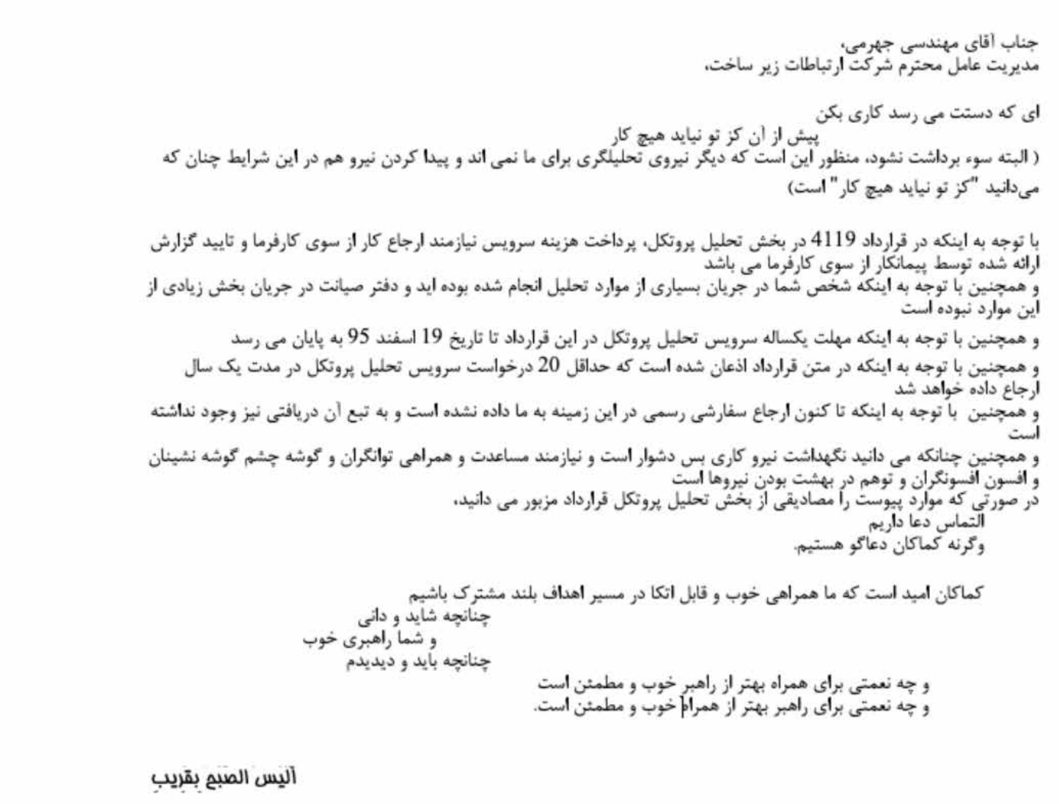
1 attachment: Proposal-Komite-Masadigh-all-13930619-10-40-final-Rezvani.docx 21.2 KB

Unread: 0 Total: 3579

The above is a picture of Abbas Aram's letter to Azari Jahormi, the then manager of the Subrahmat Company

The letter to Azari Jahormi stated that Yaftar Company was involved in protocol analysis and Internet traffic analysis, and requested additional funding from him to progress the project. The letter also mentioned that Azari Jahormi was personally aware of many cases of analysis that the protection office (the department responsible for censorship) was not aware of. The letter ended with the phrase "the path of common high goals", indicating the Yaftar company's commitment to cooperating with censorship policies. Azari Jahormi later served as the Minister of Telecommunications and

Information Technology in the second government of Hassan Rouhani. He has faced accusations of involvement in the interrogation of prisoners in 2008.



جناب آقای مهندسی جهرمی،
مدیریت عامل محترم شرکت ارتباطات زیر ساخت،

ای که دستت می رسد کاری بکن
پیش از آن کز تو نیاید هیچ کار
(البته سوء برداشت نشود، منظور این است که دیگر نیروی تحلیلگری برای ما نمی اند و پیدا کردن نیرو هم در این شرایط چنان که
می‌دانید "کز تو نیاید هیچ کار" است)

با توجه به اینکه در قرارداد 4119 در بخش تحلیل پروتکل، پرداخت هزینه سرویس نیازمند ارجاع کار از سوی کارفرما و تایید گزارش
ارائه شده توسط پیمانکار از سوی کارفرما می باشد
و همچنین با توجه به اینکه شخص شما در جریان بسیاری از موارد تحلیل انجام شده بوده اید و دفتر صیانت در جریان بخش زیادی از
این موارد نبوده است
و همچنین با توجه به اینکه مهلت یکساله سرویس تحلیل پروتکل در این قرارداد تا تاریخ 19 اسفند 95 به پایان می رسد
و همچنین با توجه به اینکه در متن قرارداد اذعان شده است که حداقل 20 درخواست سرویس تحلیل پروتکل در مدت یک سال
ارجاع داده خواهد شد
و همچنین با توجه به اینکه تا کنون ارجاع سفارشی رسمی در این زمینه به ما داده نشده است و به تبع آن دریافتی نیز وجود نداشته
است
و همچنین چنانکه می دانید نگهداشت نیرو کاری بس دشوار است و نیازمند مساعدت و همراهی توانگران و گوشه چشم گوشه نشینان
و افسون افسونگران و توهم در بهشت بودن نیروها است
در صورتی که موارد پیوست را مصادیقی از بخش تحلیل پروتکل قرارداد مزبور می دانید،
التماس دعا داریم
وگرنه کماکان دعاگو هستیم.

کماکان امید است که ما همراهی خوب و قابل اتکا در مسیر اهداف بلند مشترک باشیم
چنانچه شاید و دانی
و شما راهبری خوب
چنانچه باید و دیدیدم
و چه نعمتی برای همراه بهتر از راهبر خوب و مطمئن است
و چه نعمتی برای راهبر بهتر از همراه خوب و مطمئن است.

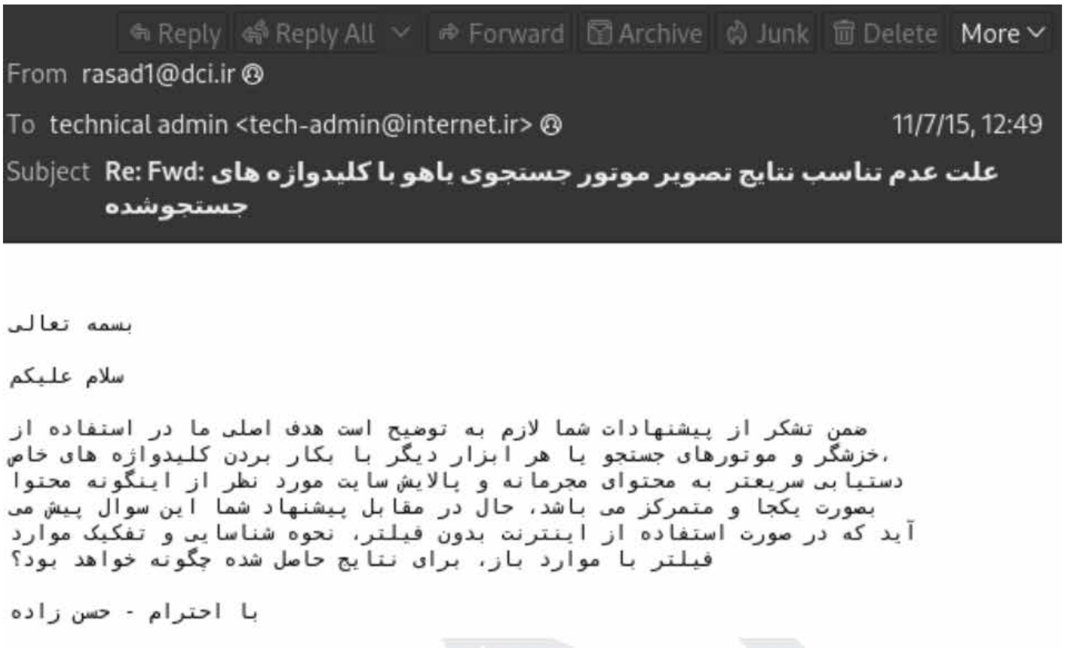
آلیس الصبح بقریب

The above is a letter sent from Yaftar Company to Azari Jahormi regarding Iran's Internet traffic analysis

Taris

The emails show that Yaftar has developed and deployed a system called Taris for the Attorney General's Office. This is a system that crawls search engines like Google and Bing, using specific keywords stored in a database and leveraging the APIs provided by these global platforms. The purpose of this system is to automatically detect and censor visual and textual content that is considered "criminal" according to the Attorney General's Office's criteria.

In an email addressed to the technical manager of the Attorney General's Office, a person named Hassanzadeh stated that the main goal of using a crawler, search engines or any other tool with specific keywords, is to access criminal content faster and cleanse the relevant website from such content in a centralized and consolidated manner. He also raised a question about how to identify and differentiate filtered and unfiltered items when accessing the Internet without a filter.



From rasad1@dci.ir

To technical admin <tech-admin@internet.ir>

11/7/15, 12:49

Subject Re: Fwd: علت عدم تناسب نتایج تصویر موتور جستجوی یاهو با کلیدواژه های جستجوشده

بسمه تعالی

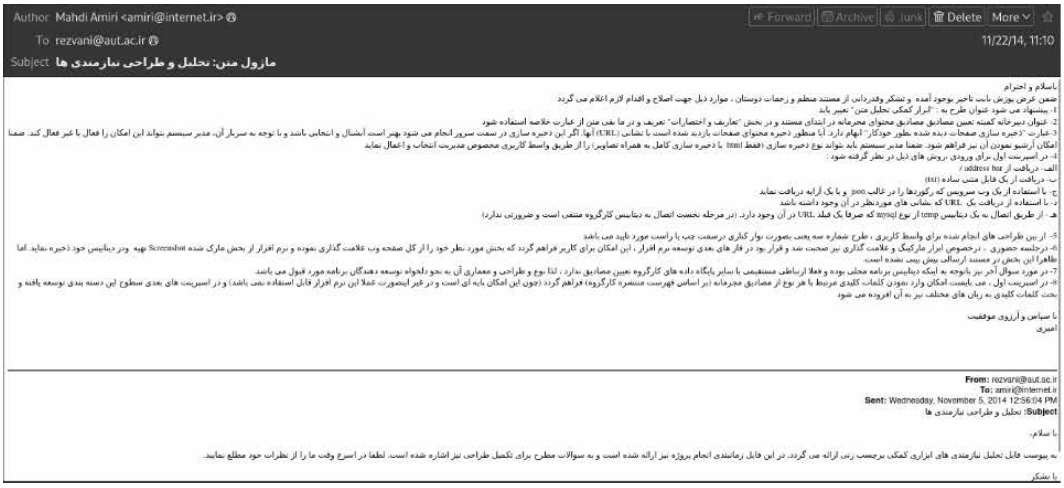
سلام علیکم

ضمن تشکر از پیشنهادات شما لازم به توضیح است هدف اصلی ما در استفاده از
خزشگر و موتورهای جستجو یا هر ابزار دیگر با بکار بردن کلیدواژه های خاص،
دستیابی سریعتر به محتوای مجرمانه و پالایش سایت مورد نظر از اینگونه محتوا
بصورت یکجا و متمرکز می باشد، حال در مقابل پیشنهاد شما این سوال پیش می
آید که در صورت استفاده از اینترنت بدون فیلتر، نحوه شناسایی و تفکیک موارد
فیلتر با موارد باز، برای نتایج حاصل شده چگونه خواهد بود؟

با احترام - حسن زاده

Text Analysis Tool

The Yaftar company is also engaged in another project with the Attorney General's Office called the "text analysis project." Within an email discussing this specific project, we discovered the presence of a PDF file that was sent to Amiri, marked with a confidential designation.



Author Mahdi Amiri <amiri@internet.ir>

To rezvani@aut.ac.ir

11/22/14, 11:10

Subject مازول متن: تحلیل و طراحی نیازمندی ها

باسلام و احترام
ضمن عرض پوزش بابت تاخیر بوجود آمده و تشکر وقدردانی از مستند منظم و زحمات دوستان ، موارد ذیل جهت اصلاح و اقدام لازم اعلام می گردد
1- پیشنهاد می شود عنوان طرح به : "ابزار کمکی تحلیل متن" تغییر یابد
2- عنوان دبیرخانه کمیته تعیین مصادیق مصادیق محتوای مجرمانه در ابتدای مستند و در بخش "تعاریف و اختصارات" تعریف و در ما بقی متن از عبارت خلاصه استفاده شود
3-عبارت "ذخیره سازی صفحات دیده شده بطور خودکار" ابهام دارد. آیا منظور ذخیره محتوای صفحات بازدید شده است با نشانی (URL) آنها. اگر این ذخیره سازی در سمت سرور انجام می شود بهتر است آپشنال و انتخابی باشد و با توجه به سربار آن، مدیر سیستم بتواند این امکان را فعال یا غیر فعال کند. ضمنا
امکان آرشیو نمودن آن نیز فراهم شود. ضمنا مدیر سیستم باید بتواند نوع ذخیره سازی (فقط html یا ذخیره سازی کامل به همراه تصاویر) را از طریق واسط کاربری مخصوص مدیریت انتخاب و اعمال نماید
4- در اسپرینت اول برای ورودی ،روش های ذیل در نظر گرفته شود :
الف- دریافت از address bar /
ب- دریافت از یک فایل متنی ساده (txt)
ج- با استفاده از یک وب سرویس که رکوردها را در قالب json و یا یک آرایه دریافت نماید
د- با استفاده از دریافت یک URL که نشانی های موردنظر در آن وجود داشته باشد
هـ - از طریق اتصال به یک دیتابیس temp از نوع mysql که صرفا یک فیلد URL در آن وجود دارد. (در مرحله نخست اتصال به دیتابیس کارگروه منتفی است و ضرورتی ندارد)

5- از بین طراحی های انجام شده برای واسط کاربری ، طرح شماره سه یعنی بصورت نوار کاری درسمت چپ یا راست مورد تایید می باشد
6- درجلسه حضوری ، درخصوص ابزار مارکینگ و علامت گذاری نیز صحبت شد و قرار بود در فاز های بعدی توسعه نرم افزار ، این امکان برای کاربر فراهم گردد که بخش مورد نظر خود را از کل صفحه وب علامت گذاری نموده و نرم افزار از بخش مارک شده Screenshot تهیه ودر دیتابیس خود ذخیره نماید. اما
ظاهرا این بخش در مستند ارسالی پیش بینی نشده است.
7- در مورد سوال آخر نیز باتوجه به اینکه دیتابیس برنامه محلی بوده و فعلا ارتباطی مستقیمی با سایر پایگاه داده های کارگروه تعیین مصادیق ندارد ، لذا نوع و طراحی و معماری آن به نحو دلخواه توسعه دهندگان برنامه مورد قبول می باشد.
8- در اسپرینت اول ، می بایست امکان وارد نمودن کلمات کلیدی مرتبط با هر نوع از مصادیق مجرمانه (بر اساس فهرست منتشره کارگروه) فراهم گردد (چون این امکان پایه ای است و در غیر اینصورت عملا این نرم افزار قابل استفاده نمی باشد) و در اسپرینت های بعدی سطوح این دسته بندی توسعه یافته و
بحث کلمات کلیدی به زبان های مختلف نیز به آن افزوده می شود

با سپاس و آرزوی موفقیت
امیری

From: rezvani@aut.ac.ir
To: amiri@internet.ir
Sent: Wednesday, November 5, 2014 12:56:04 PM
Subject: تحلیل و طراحی نیازمندی ها

با سلام،

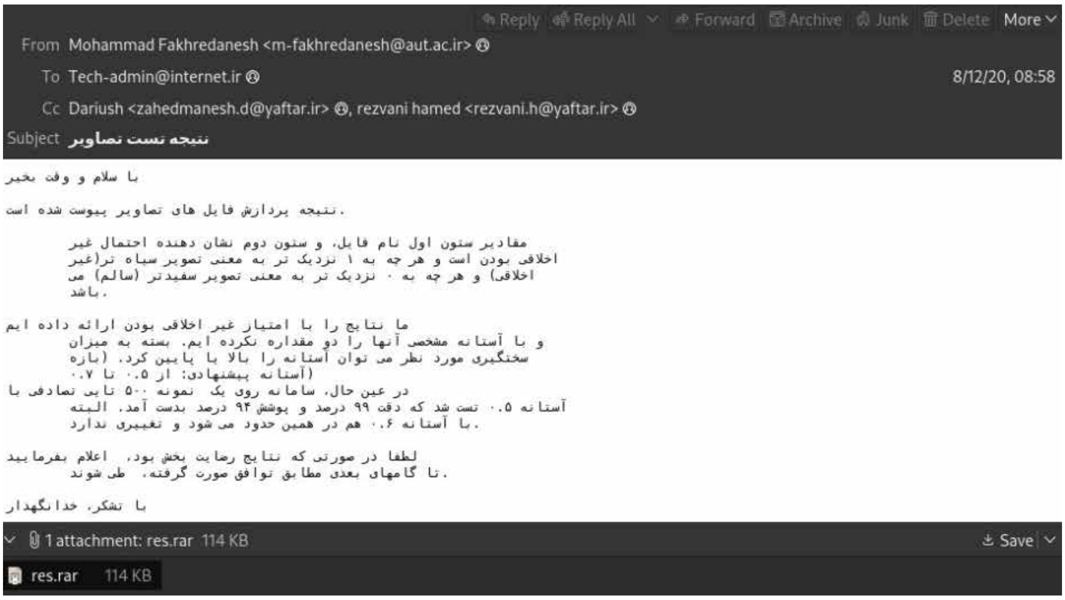
به پیوست فایل تحلیل نیازمندی های ابزاری کمکی برچسب زنی ارائه می گردد. در این فایل زمانبندی انجام پروژه نیز ارائه شده است و به سوالات مطرح برای تکمیل طراحی نیز اشاره شده است. لطفا در اسرع وقت ما را از نظرات خود مطلع نمایید.

با تشکر

This project is a Firefox add-on capable of extracting the website address from the browser, determining the language of the displayed text, and conducting text analysis according to criteria outlined by the Attorney General's Office.

Image Processing

One of the emails included the submission of image file processing results as a sample work by an individual Mohammad Fakhredanesh, who used an email account affiliated with Amirkabir University. The results were sent to the Attorney General's Office for review.

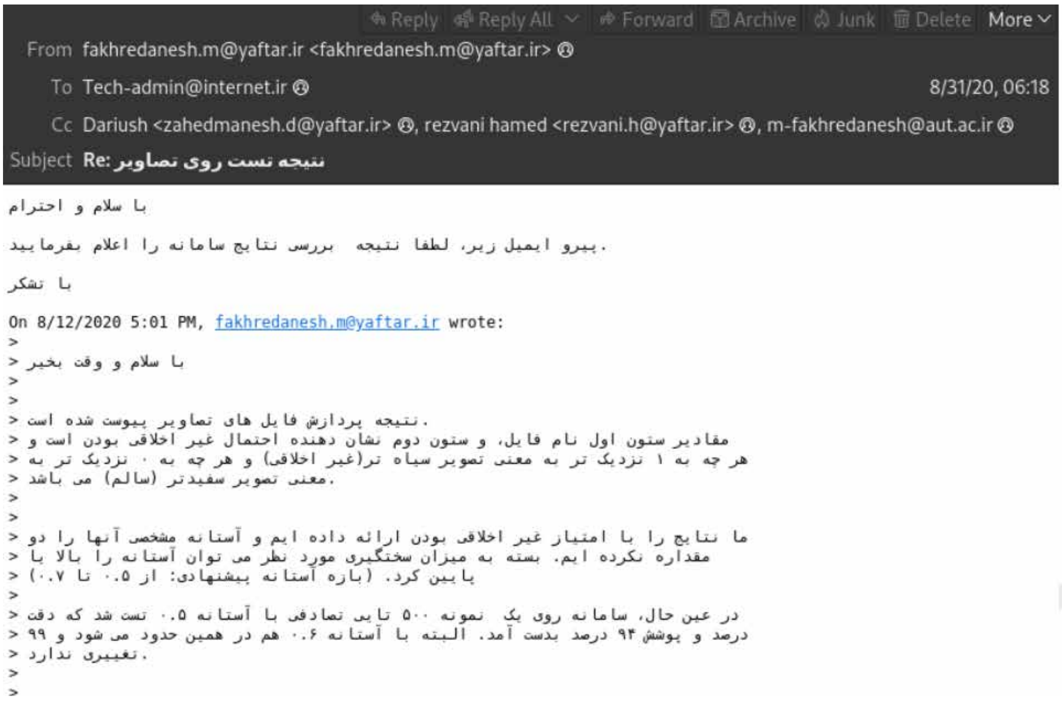


From Mohammad Fakhredanesh <m-fakhredanesh@aut.ac.ir>
To Tech-admin@internet.ir
8/12/20, 08:58
Cc Dariush <zahedmanesh.d@yaftar.ir>, rezvani hamed <rezvani.h@yaftar.ir>
Subject نتیجه تست تصاویر

```
با سلام و وقت بخیر

نتیجه پردازش فایل های تصاویر پیوست شده است.

        مقادیر ستون اول نام فایل، و ستون دوم نشان دهنده احتمال غیر
        اخلاقی بودن است و هر چه به ۱ نزدیک تر به معنی تصویر سیاه تر(غیر
        اخلاقی) و هر چه به ۰ نزدیک تر به معنی تصویر سفیدتر (سالم) می
        باشد.

ما نتایج را با امتیاز غیر اخلاقی بودن ارائه داده ایم
        و با آستانه مشخص آنها را دو مقداره نکرده ایم. بسته به میزان
        سختگیری مورد نظر می توان آستانه را بالا یا پایین کرد. (بازه
        آستانه پیشنهادی: از ۰.۵ تا ۰.۷)
در عین حال، سامانه روی یک  نمونه ۵۰۰ تایی تصادفی با
        آستانه ۰.۵ تست شد که دقت ۹۹ درصد و پوشش ۹۴ درصد بدست آمد. البته
        با آستانه ۰.۶ هم در همین حدود می شود و تغییری ندارد.

لطفا در صورتی که نتایج رضایت بخش بود، اعلام بفرمایید
        تا گامهای بعدی مطابق توافق صورت گرفته، طی شوند.

با تشکر، خدانگهدار
```

1 attachment: res.rar 114 KB
res.rar 114 KB

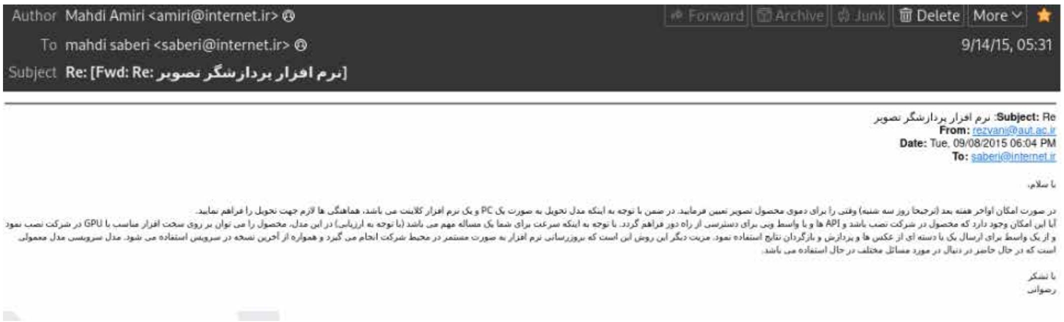
In the same email thread, Mohammad Fakhredanesh received a subsequent email from the Douran company, seeking a response from the Attorney General's Office regarding the aforementioned subject.



From fakhredanesh.m@yaftar.ir <fakhredanesh.m@yaftar.ir>
To Tech-admin@internet.ir
8/31/20, 06:18
Cc Dariush <zahedmanesh.d@yaftar.ir>, rezvani hamed <rezvani.h@yaftar.ir>, m-fakhredanesh@aut.ac.ir
Subject Re: نتیجه تست روی تصاویر

```
با سلام و احترام

پیرو ایمیل زیر، لطفا نتیجه  بررسی نتایج سامانه را اعلام بفرمایید.

با تشکر

On 8/12/2020 5:01 PM, fakhredanesh.m@yaftar.ir wrote:
>
> با سلام و وقت بخیر
>
>
> نتیجه پردازش فایل های تصاویر پیوست شده است.
> مقادیر ستون اول نام فایل، و ستون دوم نشان دهنده احتمال غیر اخلاقی بودن است و
> هر چه به ۱ نزدیک تر به معنی تصویر سیاه تر(غیر اخلاقی) و هر چه به ۰ نزدیک تر به
> معنی تصویر سفیدتر (سالم) می باشد.
>
>
> ما نتایج را با امتیاز غیر اخلاقی بودن ارائه داده ایم و آستانه مشخص آنها را دو
> مقداره نکرده ایم. بسته به میزان سختگیری مورد نظر می توان آستانه را بالا یا
> پایین کرد. (بازه آستانه پیشنهادی: از ۰.۵ تا ۰.۷)
>
> در عین حال، سامانه روی یک  نمونه ۵۰۰ تایی تصادفی با آستانه ۰.۵ تست شد که دقت
> ۹۹ درصد و پوشش ۹۴ درصد بدست آمد. البته با آستانه ۰.۶ هم در همین حدود می شود و
> تغییری ندارد.
>
>
```

Upon further investigation, we discovered that Yaftar company has engaged in collaborations and projects related to image processing in partnership with Iran's Attorney General's Office. The project in question is titled, "Analysis of requirements and presentation of a schedule for the development of a tool for detecting inappropriate images of the Criminal Instances Committee."



Author Mahdi Amiri <amiri@internet.ir>
To mahdi saberi <saberi@internet.ir>
9/14/15, 05:31
Subject Re: [Fwd: Re: نرم افزار پردازشگر تصویر]

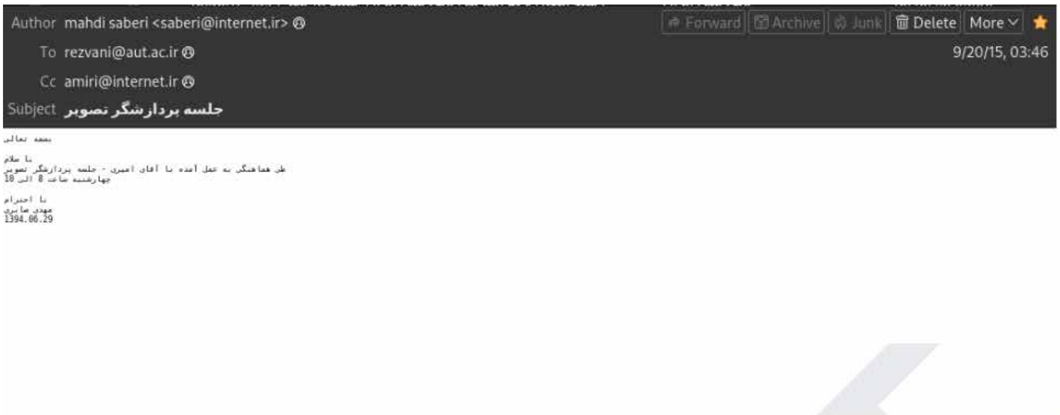
Subject: Re: نرم افزار پردازشگر تصویر
From: rezvani@aut.ac.ir
Date: Tue, 09/08/2015 06:04 PM
To: saberi@internet.ir

با سلام،

در صورت امکان اواخر هفته بعد (ترجیحا روز سه شنبه) وقتی را برای دموی محصول تصویر تعیین فرمایید. در ضمن با توجه به اینکه مدل تحویل به صورت یک PC و یک نرم افزار کلاینت می باشد، هماهنگی ها لازم جهت تحویل را فراهم نمایید.
آیا این امکان وجود دارد که محصول در شرکت نصب باشد و API ها و یا واسط وبی برای دسترسی از راه دور فراهم گردد. با توجه به اینکه سرعت برای شما یک مساله مهم می باشد (با توجه به ارزیابی) در این مدل، محصول را می توان بر روی سخت افزار مناسب با GPU در شرکت نصب نمود
و از یک واسط برای ارسال یک یا دسته ای از عکس ها و پردازش و بازگردان نتایج استفاده نمود. مزیت دیگر این روش این است که بروزرسانی نرم افزار به صورت مستمر در محیط شرکت انجام می گیرد و همواره از آخرین نسخه در سرویس استفاده می شود. مدل سرویس مدل معمولی
است که در حال حاضر در دنبال در مورد مسائل مختلف در حال استفاده می باشد.

با تشکر
رضوانی

Numerous emails indicate the use of an email address associated with Hamed Rizvani, affiliated with Amirkabir University. It appears that a significant portion of the company's activities were conducted by researchers who were studying at this university.

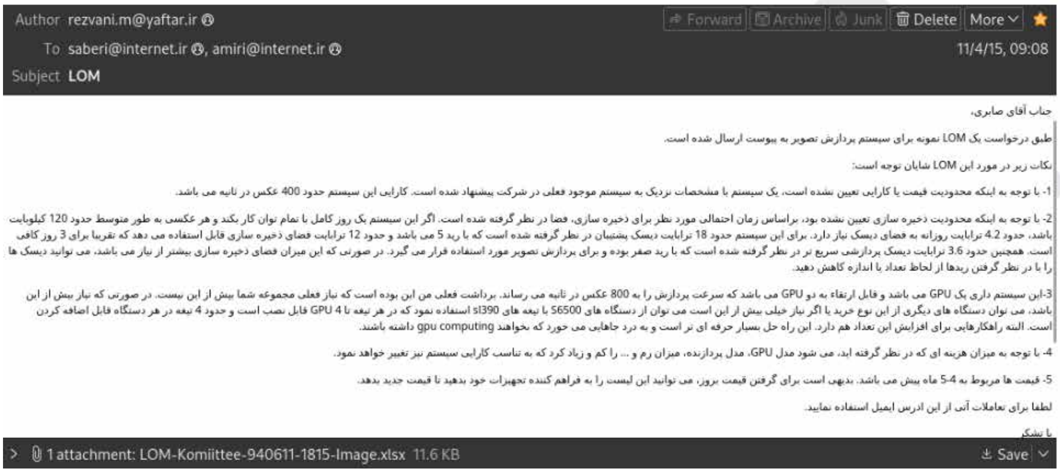


Author mahdi saberi <saberi@internet.ir>
To rezvani@aut.ac.ir
Cc amiri@internet.ir
9/20/15, 03:46
Subject جلسه پردازشگر تصویر

بسمه تعالی

با سلام
طی هماهنگی به عمل آمده با آقای امیری - جلسه پردازشگر تصویر
چهارشنبه ساعت 8 الی 10

با احترام
مهدی صابری
1394.06.29



Author rezvani.m@yaftar.ir
To saberi@internet.ir, amiri@internet.ir
11/4/15, 09:08
Subject LOM

جناب آقای صابری،

طبق درخواست یک LOM نمونه برای سیستم پردازش تصویر به پیوست ارسال شده است.

نکات زیر در مورد این LOM شایان توجه است:

1- با توجه به اینکه محدودیت قیمت یا کارایی تعیین نشده است، یک سیستم با مشخصات نزدیک به سیستم موجود فعلی در شرکت پیشنهاد شده است. کارایی این سیستم حدود 400 عکس در ثانیه می باشد.

2- با توجه به اینکه محدودیت ذخیره سازی تعیین نشده بود، براساس زمان احتمالی مورد نظر برای ذخیره سازی، فضا در نظر گرفته شده است. اگر این سیستم یک روز کامل با تمام توان کار بکند و هر عکسی به طور متوسط حدود 120 کیلوبایت باشد، حدود 4.2 ترابایت روزانه به فضای دیسک نیاز دارد. برای این سیستم حدود 18 ترابایت دیسک پشتیبان در نظر گرفته شده است که با رید 5 می باشد و حدود 12 ترابایت فضای ذخیره سازی قابل استفاده می دهد که تقریبا برای 3 روز کافی است. همچنین حدود 3.6 ترابایت دیسک پردازشی سریع تر در نظر گرفته شده است که با رید صفر بوده و برای پردازش تصویر مورد استفاده قرار می گیرد. در صورتی که این میزان فضای ذخیره سازی بیشتر از نیاز می باشد، می توانید دیسک ها را با در نظر گرفتن ریدها از لحاظ تعداد یا اندازه کاهش دهید.

3-این سیستم داری یک GPU می باشد و قابل ارتقاء به دو GPU می باشد که سرعت پردازش را به 800 عکس در ثانیه می رساند. برداشت فعلی من این بوده است که نیاز فعلی مجموعه شما بیش از این نیست. در صورتی که نیاز بیش از این باشد، می توان دستگاه های دیگری از این نوع خرید یا اگر نیاز خیلی بیش از این است می توان از دستگاه های S6500 با تیغه های sl390 استفاده نمود که در هر تیغه تا 4 GPU قابل نصب است و حدود 4 تیغه در هر دستگاه قابل اضافه کردن است. البته راهکارهایی برای افزایش این تعداد هم دارد. این راه حل بسیار حرفه ای تر است و به درد جاهایی می خورد که بخواهند gpu computing داشته باشند.

4- با توجه به میزان هزینه ای که در نظر گرفته اید، می شود مدل GPU، مدل پردازنده، میزان رم و ... را کم و زیاد کرد که به تناسب کارایی سیستم نیز تغییر خواهد نمود.

5- قیمت ها مربوط به 4-5 ماه پیش می باشد. بدیهی است برای گرفتن قیمت بروز، می توانید این لیست را به فراهم کننده تجهیزات خود بدهید تا قیمت جدید بدهد.

لطفا برای تعاملات آتی از این ادرس ایمیل استفاده نمایید.

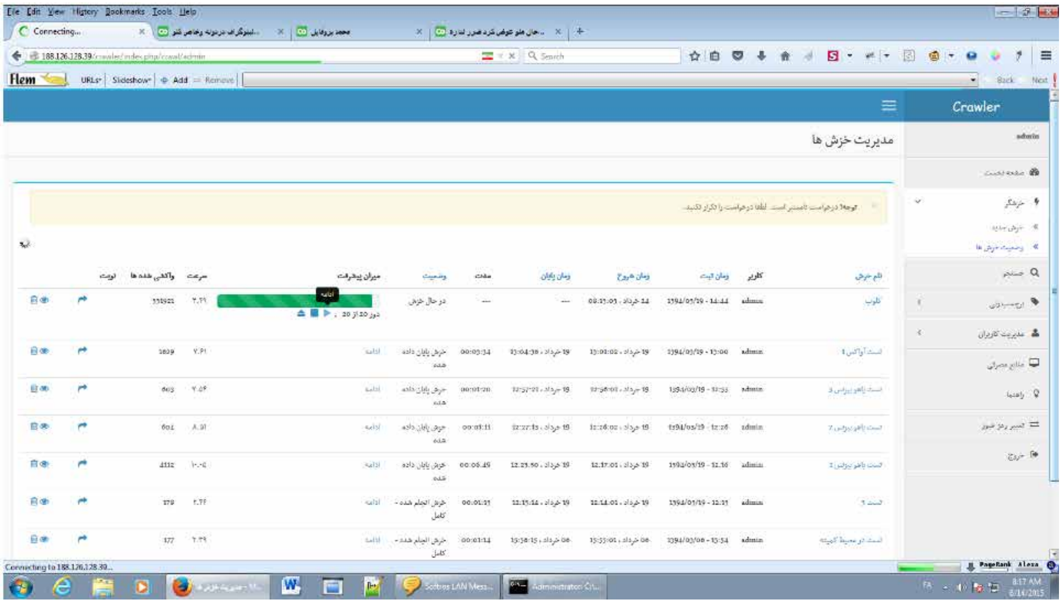
با تشکر

1 attachment: LOM-Komiittee-940611-1815-Image.xlsx 11.6 KB

Identification of Bad Hejab and Nudity

The emails show that Yaftar has been working on a project to identify instances of "unethical" content in images using intelligent methods. Abbas Aram has claimed responsibility for overseeing the project on behalf of Hamed Rizvani, the company's director. In an email, Aram sent a file containing three assistant tools designed for identifying instances of criminal content on web pages, upload centers, and images. The emails also included images showcasing the user interface of this program.

Additionally, the emails revealed a document containing a questionnaire sent by the company to the Attorney General's Office. The purpose of the questionnaire was to gain a better understanding of the specific needs of the Attorney General's Office regarding women's clothing and body parts. The document stated, "Declaration answers for exploitation in order to design smart software for cyberspace monitoring and do not cover all the examples and criteria desired by the working group to filter criminal content."



مدیریت خزش ها

توجه! درخواست نامعتبر است. لطفا درخواست را تکرار کنید.

نام خزش	کاربر	زمان ثبت	زمان شروع	زمان پایان	مدت	وضعیت	میزان پیشرفت	سرعت	واکشی شده ها	نوبت
ناوب	admin	1394/03/19 - 14:44	24 خرداد ، 08:35:03	---	---	در حال خزش	دور 20 از 20	۲.۲۱	331921	
تست آواکس 1	admin	1394/03/19 - 13:00	19 خرداد ، 13:01:02	19 خرداد ، 13:04:36	00:03:34	خزش پایان داده شده	ادامه	۷.۶۱	1629	
تست یاهو پرپرس 3	admin	1394/03/19 - 12:55	19 خرداد ، 12:56:01	19 خرداد ، 12:57:21	00:01:20	خزش پایان داده شده	ادامه	۷.۵۴	603	
تست یاهو پرپرس 2	admin	1394/03/19 - 12:26	19 خرداد ، 12:26:02	19 خرداد ، 12:27:13	00:01:11	خزش پایان داده شده	ادامه	۸.۱۱	601	
تست یاهو پرپرس 1	admin	1394/03/19 - 12.16	19 خرداد ، 12.17:01	19 خرداد ، 12.23.50	00:06.49	خزش پایان داده شده	ادامه	۱۰.۰۶	4112	
تست 3	admin	1394/03/19 - 12:13	19 خرداد ، 12:14:01	19 خرداد ، 12:15:14	00:01:13	خزش انجام شده - کامل	ادامه	۲.۲۴	379	
تست در محیط کمیته	admin	1394/03/08 - 15:54	08 خرداد ، 15:55:01	08 خرداد ، 15:56:15	00:01:14	خزش انجام شده - کامل	ادامه	۲.۳۹	377	

The photo of crawler application obtained from the emails of the prosecutor's office

The questionnaire included questions such as:

1. What are the guidelines or restrictions regarding women's clothing? This may include considerations such as Sharia law, the type of clothing worn by women in IRIB (Islamic Republic of Iran Broadcasting), and the type of clothing worn by women in society.

2. In the process of refining the photos and establishing boundaries,

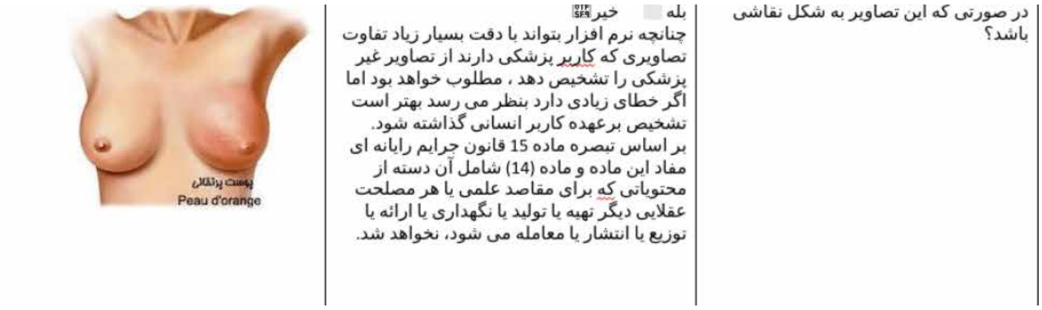
does the nationality of the people in the photos, whether they are Iranian or foreign, have any influence? Specifically, the question arises as to whether there is a distinction between photos of two women, one Iranian and the other foreign, when they are under completely identical conditions. If the answer is yes, how should this difference be taken into account and applied?

3. Are there any specific guidelines or considerations for pictures that display a particular part of the body, such as the chest, with the purpose of demonstrating a medical condition?

4. What if these images are in the form of paintings?

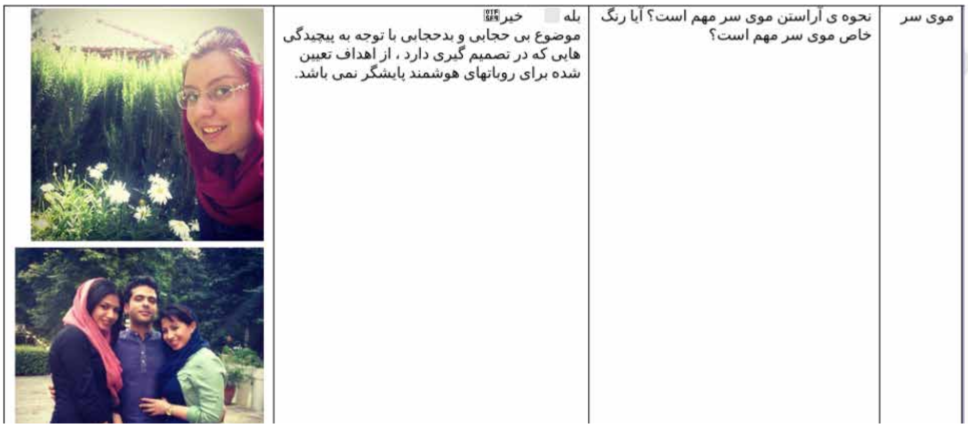
5. Is there any issue with a photograph of a woman wearing regular attire typically worn at home, as long as her hands are visible up to the elbows, the neckline is modest, and her hair is clearly visible without any excessive makeup?

These questions delve into specific details regarding each body part and inquire about how they should be covered to meet the desired criteria outlined by the Attorney General's Office. Additionally, some questions included sample photos to further illustrate the specific cases being discussed.



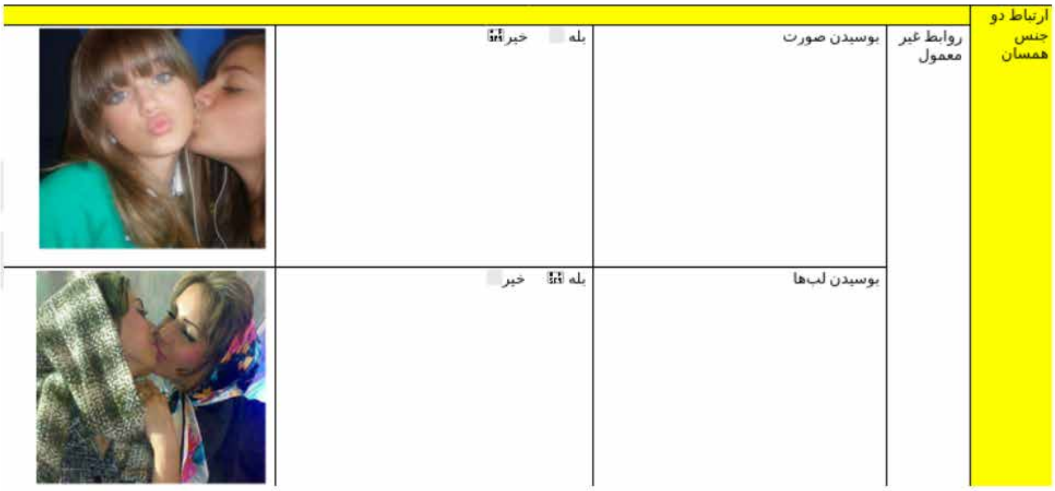
	بله □ خیر ☒ چنانچه نرم افزار بتواند با دقت بسیار زیاد تفاوت تصاویری که کاربر پزشکی دارند از تصاویر غیر پزشکی را تشخیص دهد ، مطلوب خواهد بود اما اگر خطای زیادی دارد بنظر می رسد بهتر است تشخیص برعهده کاربر انسانی گذاشته شود. بر اساس تبصره ماده 15 قانون جرایم رایانه ای مفاد این ماده و ماده (14) شامل آن دسته از محتویاتی که برای مقاصد علمی یا هر مصلحت عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا توزیع یا انتشار یا معامله می شود، نخواهد شد.	در صورتی که این تصاویر به شکل نقاشی باشد؟

An example of dealing with a medical image



	بله □ خیر ☒ موضوع بی حجابی و بدحجابی با توجه به پیچیدگی هایی که در تصمیم گیری دارد ، از اهداف تعیین شده برای روباتهای هوشمند پایشگر نمی باشد.	نحوه ی آراستن موی سر مهم است؟ آیا رنگ خاص موی سر مهم است؟	موی سر

An example of how to deal with the image of "bad hijab"



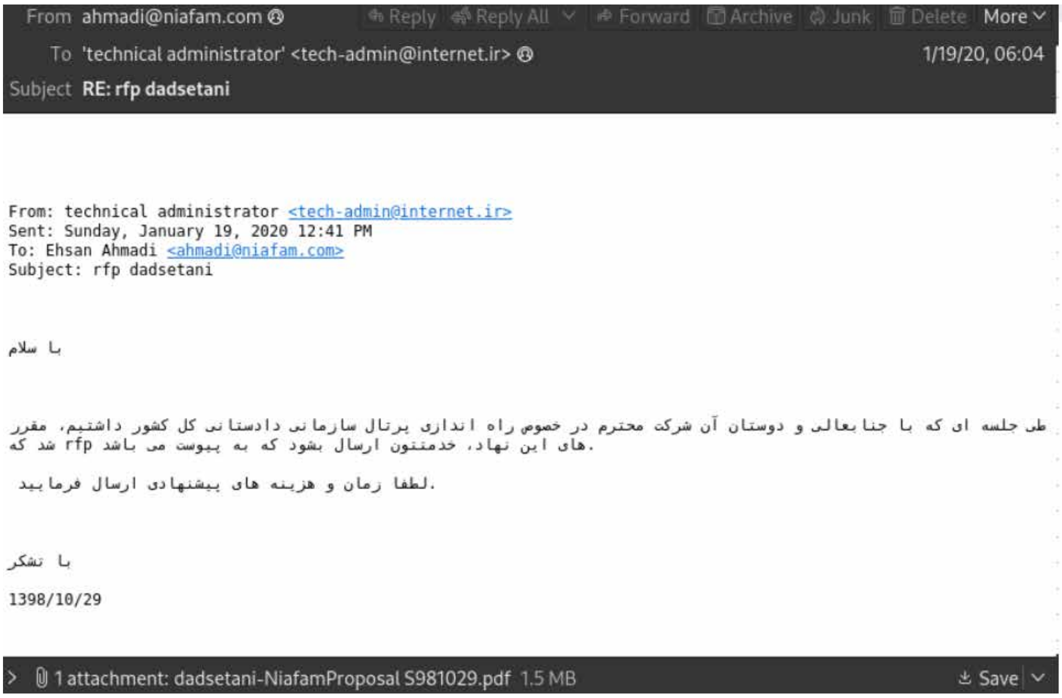
ارتباط دو جنس همسان	روابط غیر معمول	بوسیدن صورت	بله □ خیر ☒
		بوسیدن لب‌ها	بله ☒ خیر □

An example of the method of dealing with the image of "same-sex sexual relations"

Niafam

The emails from Niafam company reveal their willingness to cooperate with the Attorney General's Office to launch an organizational portal with special capabilities (link to the archived version of the company's website). The proposed features include facial recognition and identification of individuals depicted in news images, aimed at enhancing the generated content. Additionally, the company's request for proposal (RFP) submitted to the Attorney General's Office mentions the ability to tag names of individuals on the website. For further details and visual reference, a video demonstrating these features is provided on the archived version of the company's website. In the RFP, which was sent as a PDF file to the Attorney General's Office, the section on leveraging artificial intelligence outlines various capabilities.

In the RFP, which was sent as a PDF file to the Attorney General's Office, the section on leveraging artificial intelligence outlines various capabilities. These include facial recognition from both images and videos, precise indexing of individuals' images in Google, and other image processing-related functionalities.



From ahmadi@niafam.com
To 'technical administrator' <tech-admin@internet.ir>
Subject RE: rfp dadsetani
1/19/20, 06:04

From: technical administrator <tech-admin@internet.ir>
Sent: Sunday, January 19, 2020 12:41 PM
To: Ehsan Ahmadi <ahmadi@niafam.com>
Subject: rfp dadsetani

با سلام

طی جلسه ای که با جنابعالی و دوستان آن شرکت محترم در خصوص راه اندازی پرتال سازمانی دادستانی کل کشور داشتیم، مقرر شد که rfp های این نهاد، خدمتتون ارسال بشود که به پیوست می باشد.

لطفا زمان و هزینه های پیشنهادی ارسال فرمایید.

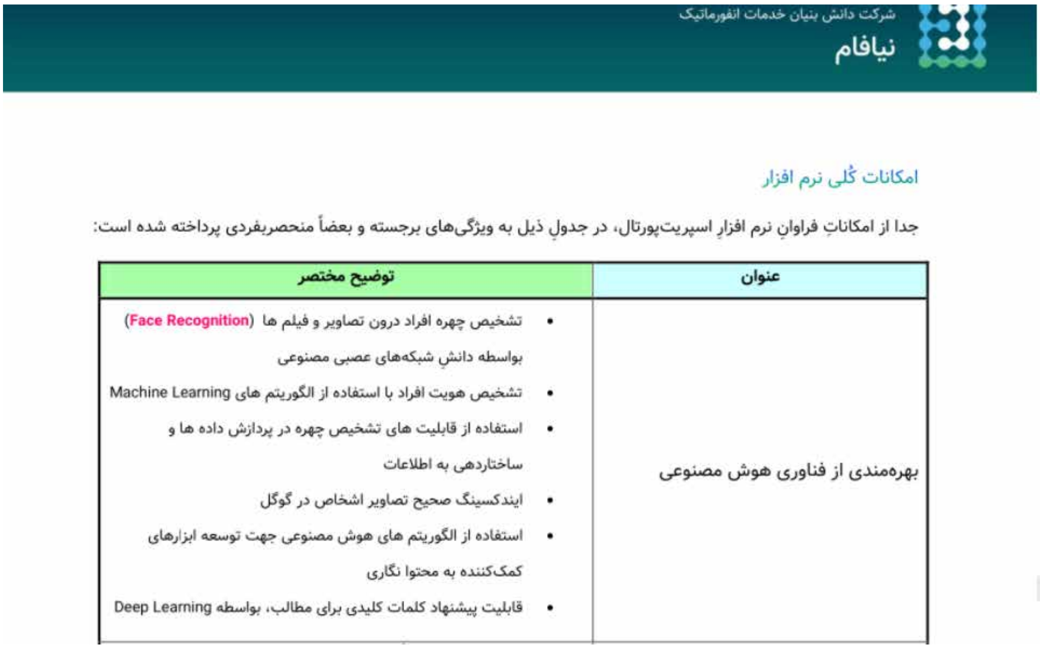
با تشکر

1398/10/29

1 attachment: dadsetani-NiafamProposal S981029.pdf 1.5 MB

The image of the proposal that explains the capabilities of this company's artificial intelligence system, including facial recognition

Facial recognition technology is increasingly mentioned by Iranian authorities as a tool for identifying and suppressing dissidents. Mohammad Saleh Hashemi Golpayegani, the Secretary of the Headquarters for Promotion of Virtue and Prevention of Vice, said in an interview with Khabar Fori on September 4, 2022, that the organization uses facial recognition technology to identify what he described as "improper and deviant behavior" and unveilings. He said the image of "delinquent citizens" is compared to the image stored in the national ID database, and ultimately the person's identity is verified, followed by legal actions such as fines or arrests.

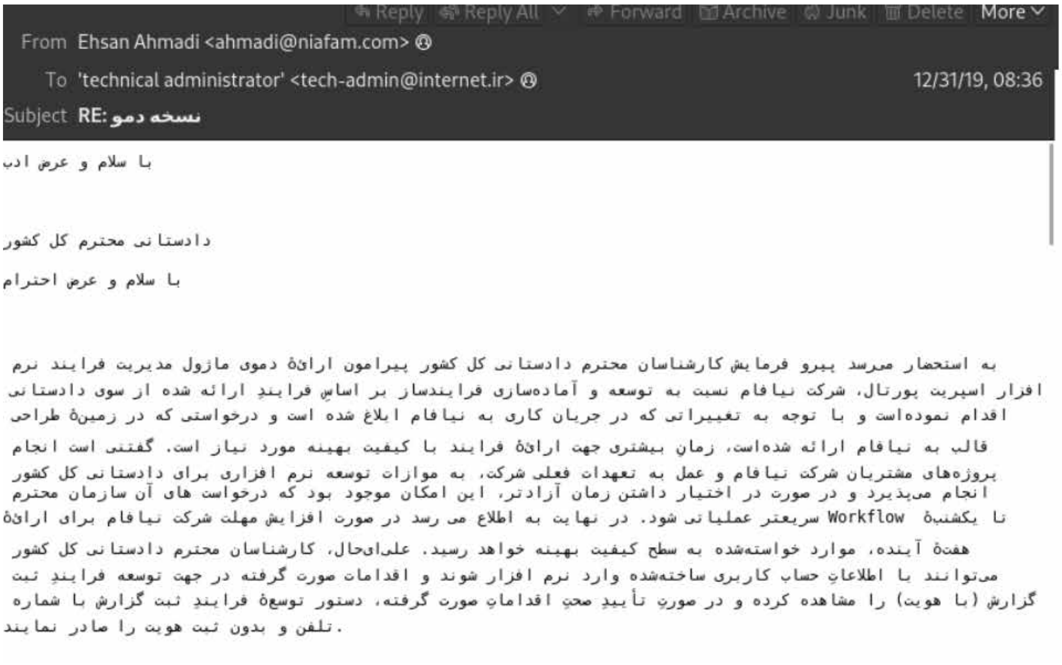


شرکت دانش بنیان خدمات انفورماتیک
نیافام

امکانات کُلی نرم افزار

جدا از امکاناتِ فراوانِ نرم افزارِ اسپریت‌پورتال، در جدولِ ذیل به ویژگی‌های برجسته و بعضاً منحصربفردی پرداخته شده است:

عنوان	توضیح مختصر
بهره‌مندی از فناوری هوش مصنوعی	• تشخیص چهره افراد درون تصاویر و فیلم ها (Face Recognition) بواسطه دانش شبکه‌های عصبی مصنوعی • تشخیص هویت افراد با استفاده از الگوریتم های Machine Learning • استفاده از قابلیت های تشخیص چهره در پردازش داده ها و ساختاردهی به اطلاعات • ایندکسینگ صحیح تصاویر اشخاص در گوگل • استفاده از الگوریتم های هوش مصنوعی جهت توسعه ابزارهای کمک‌کننده به محتوا نگاری • قابلیت پیشنهاد کلمات کلیدی برای مطالب، بواسطه Deep Learning



From Ehsan Ahmadi <ahmadi@niafam.com>
To 'technical administrator' <tech-admin@internet.ir>
12/31/19, 08:36
Subject RE: نسخه دمو

با سلام و عرض ادب

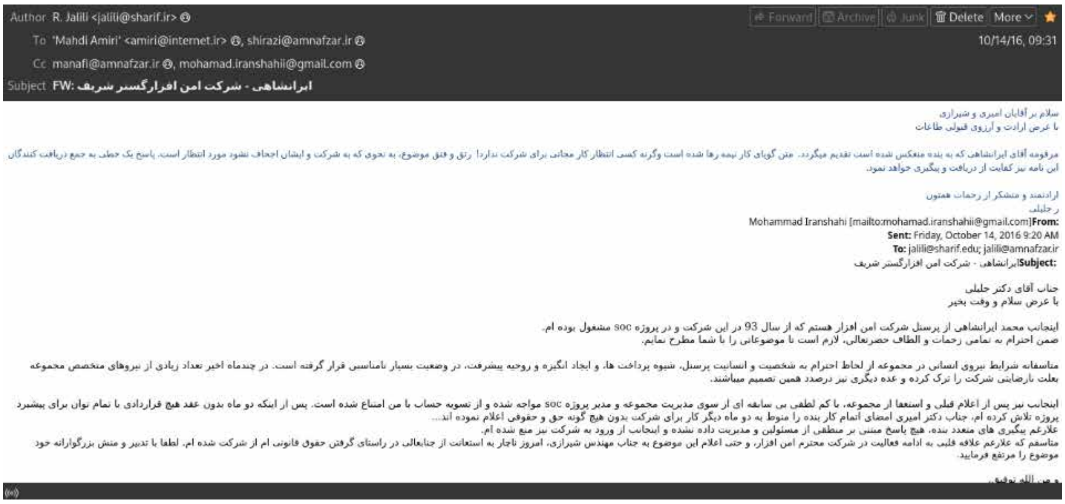
دادستانی محترم کل کشور

با سلام و عرض احترام

به استحضار میرسد پیرو فرمایش کارشناسان محترم دادستانی کل کشور پیرامون ارائهٔ دموی ماژول مدیریت فرایند نرم
افزار اسپریت پورتال، شرکت نیافام نسبت به توسعه و آماده‌سازی فرایندساز بر اساسِ فرایندِ ارائه شده از سوی دادستانی
اقدام نموده‌است و با توجه به تغییراتی که در جریان کاری به نیافام ابلاغ شده است و درخواستی که در زمینهٔ طراحی
قالب به نیافام ارائه شده‌است، زمانِ بیشتری جهت ارائهٔ فرایند با کیفیت بهینه مورد نیاز است. گفتنی است انجام
پروژه‌های مشتریان شرکت نیافام و عمل به تعهدات فعلی شرکت، به موازات توسعه نرم افزاری برای دادستانی کل کشور
انجام می‌پذیرد و در صورت در اختیار داشتن زمان آزادتر، این امکان موجود بود که درخواست های آن سازمان محترم
تا یکشنبهٔ Workflow سریعتر عملیاتی شود. در نهایت به اطلاع می رسد در صورت افزایش مهلت شرکت نیافام برای ارائهٔ
هفتهٔ آینده، موارد خواسته‌شده به سطح کیفیت بهینه خواهد رسید. علی‌ای‌حال، کارشناسان محترم دادستانی کل کشور
می‌توانند با اطلاعاتِ حساب کاربری ساخته‌شده وارد نرم افزار شوند و اقدامات صورت گرفته در جهت توسعه فرایندِ ثبت
گزارش (با هویت) را مشاهده کرده و در صورتِ تأییدِ صحتِ اقداماتِ صورت گرفته، دستور توسعهٔ فرایندِ ثبت گزارش با شماره
تلفن و بدون ثبت هویت را صادر نمایند.

Additionally, building on the previous communications, a few months later, Ehsan Ahmadi, the chairman of the board of directors at Niafam and also the company's marketing and sales manager, sent another email titled, "Demo Version." In this email, Mr. Ahmadi specifically addressed the company's intention to reform their system based on the feedback provided by the Attorney General's Office.

Furthermore, additional emails from the company indicate that a cooperation contract has been finalized, leading to the implementation of the Attorney General's Office portal by Niafam. The exact financial amount specified in the contract remains unclear. It is worth noting that the portal's development was executed in accordance with the specified requirements outlined in the earlier mentioned RFP.



Author R. Jalili <jalili@sharif.ir>
To 'Mahdi Amiri' <amiri@internet.ir>, shirazi@amnafzar.ir
10/14/16, 09:31
Cc manafi@amnafzar.ir, mohamad.iranshahii@gmail.com
Subject FW: ایرانشاهی - شرکت امن افزارگستر شریف

سلام بر آقایان امیری و شیرازی
با عرض ارادت و آرزوی قبولی طاعات

مرقومه آقای ایرانشاهی که به بنده منعکس شده است تقدیم میگردد. متن گویای کار نیمه رها شده است وگرنه کسی انتظار کار مجانی برای شرکت ندارد! رتق و فتق موضوع، به نحوی که به شرکت و ایشان اجحاف نشود مورد انتظار است. پاسخ یک خطی به جمع دریافت کنندگان
این نامه نیز کفایت از دریافت و پیگیری خواهد نمود.

ارادتمند و متشکر از زحمات همتون
ر.جلیلی
Mohammad Iranshahi [mailto:mohamad.iranshahii@gmail.com]**From:**
Sent: Friday, October 14, 2016 9:20 AM
To: jalili@sharif.edu; jalili@amnafzar.ir
:**Subject**ایرانشاهی - شرکت امن افزارگستر شریف

جناب آقای دکتر جلیلی
با عرض سلام و وقت بخیر

اینجانب محمد ایرانشاهی از پرسنل شرکت امن افزار هستم که از سال 93 در این شرکت و در پروژه soc مشغول بوده ام.
ضمن احترام به تمامی زحمات و الطاف حضرتعالی، لازم است تا موضوعاتی را با شما مطرح نمایم.

متاسفانه شرایط نیروی انسانی در مجموعه از لحاظ احترام به شخصیت و انسانیت پرسنل، شیوه پرداخت ها، و ایجاد انگیزه و روحیه پیشرفت، در وضعیت بسیار نامناسبی قرار گرفته است. در چندماه اخیر تعداد زیادی از نیروهای متخصص مجموعه
بعلت نارضایتی شرکت را ترک کرده و عده دیگری نیز درصدد همین تصمیم میباشند.

اینجانب نیز پس از اعلام قبلی و استعفا از مجموعه، با کم لطفی بی سابقه ای از سوی مدیریت مجموعه و مدیر پروژه soc مواجه شده و از تسویه حساب با من امتناع شده است. پس از اینکه دو ماه بدون عقد هیچ قراردادی با تمام توان برای پیشبرد
پروژه تلاش کرده ام، جناب دکتر امیری امضای اتمام کار بنده را منوط به دو ماه دیگر کار برای شرکت بدون هیچ گونه حق و حقوقی اعلام نموده اند...
علارغم پیگیری های متعدد بنده، هیچ پاسخ مبتنی بر منطقی از مسئولین و مدیریت داده نشده و اینجانب از ورود به شرکت نیز منع شده ام.
متاسفم که علارغم علاقه قلبی به ادامه فعالیت در شرکت محترم امن افزار، و حتی اعلام این موضوع به جناب مهندس شیرازی، امروز ناچار به استعانت از جنابعالی در راستای گرفتن حقوق قانونی ام از شرکت شده ام. لطفا با تدبیر و منش بزرگوارانه خود
موضوع را مرتفع فرمایید.

و من الله توفیق

Amnafzar Sharif

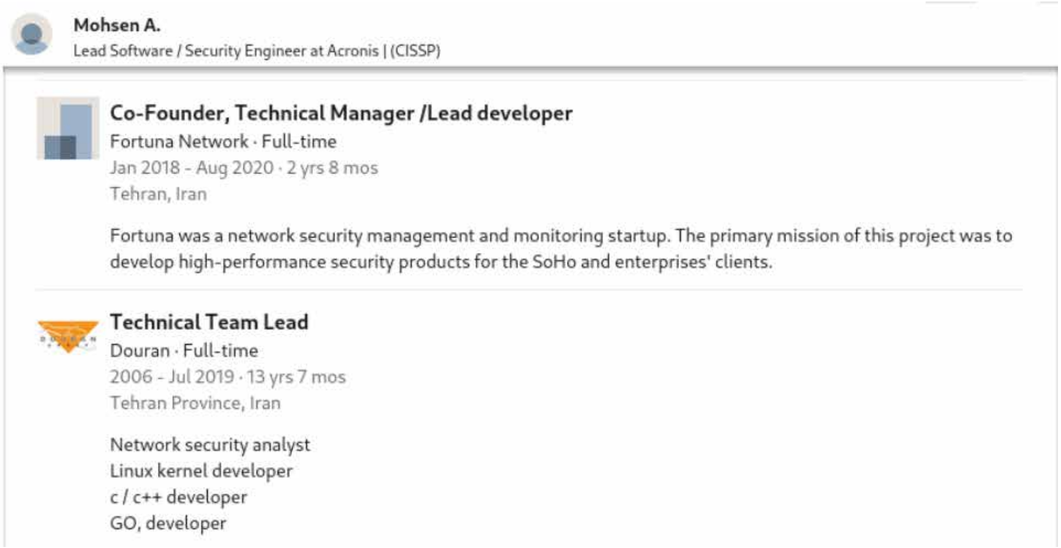
An email from an employee of Amnafzar Sharif, a company involved in Internet blocking and censoring operations, shows their discontent with their job situation. The employee forwarded their complaint to Rasul Jalili, the president of Sharif University and a member of SCC (Supreme Council of Cyberspace), and to several individuals within the Attorney General's Office. This shows the cooperation of Amnafzar Sharif with the Working Group for Determining Instances of Criminal Content.

Douran Group

The Douran Group is another Internet blocking and censoring contractor named in leaked emails. The company was sanctioned by the US Treasury Department in October 2022 for "censorship or other activities that limit the freedom of expression or assembly of the Iranian people since the June 2009 election."

According to the UK government Alireza Abedinejad, the CEO of Douran, holds a Dominican nationality and established a company in London, United Kingdom called "FOLLOW SOFT LTD" on February 26, 2020.

An anonymous source familiar with Douran told Filterwatch, "Amer Najafianpour, Alireza Abedinejad, and Mohsen Atigh, were key figures in charge of Internet blocking and censoring at Douran." Mohsen Atigh's LinkedIn page confirms his collaboration with Douran from 2006 to 2019, and shows that he is currently residing in Sofia, Bulgaria, working as a security engineer for Acronis. LinkedIn information for Douran shows that several other employees of this company reside outside of Iran.



Mohsen A.
Lead Software / Security Engineer at Acronis | (CISSP)

Co-Founder, Technical Manager /Lead developer
Fortuna Network · Full-time
Jan 2018 - Aug 2020 · 2 yrs 8 mos
Tehran, Iran

Fortuna was a network security management and monitoring startup. The primary mission of this project was to develop high-performance security products for the SoHo and enterprises' clients.

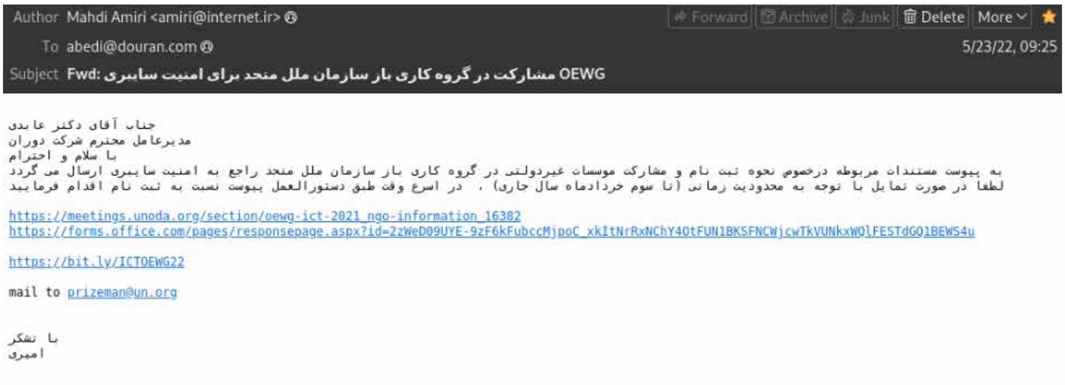
Technical Team Lead
Douran · Full-time
2006 - Jul 2019 · 13 yrs 7 mos
Tehran Province, Iran

Network security analyst
Linux kernel developer
c / c++ developer
GO, developer

On May 5, 2022, Douran Company was ordered by the Attorney General's Office, with backing from the Ministry of Foreign Affairs of Iran,to register in the United Nations Open-Ended Working Group (OEWG) on cyber security.

Development and Sale of Internet Censorship and Blocking Equipments

Douran has also established contracts with Internet providers in Iran to provide and implement censorship equipment and traffic analysis tools. These contracts also encompass support and backup services, and note that if the bandwidth requirements increase, the contract price will correspondingly increase based on factors such as port speed and switch capabilities. The contracts refer to Internet blocking and censoring activities using terms such as "protection" or "refining."



Author Mahdi Amiri <amiri@internet.ir>
To abedi@douran.com
5/23/22, 09:25
Subject Fwd: مشارکت در گروه کاری باز سازمان ملل متحد برای امنیت سایبری OEWG

جناب آقای دکتر عابدی
مدیرعامل محترم شرکت دوران
با سلام و احترام
به پیوست مستندات مربوطه درخصوص نحوه ثبت نام و مشارکت موسسات غیردولتی در گروه کاری باز سازمان ملل متحد راجع به امنیت سایبری ارسال می گردد
لطفا در صورت تمایل با توجه به محدودیت زمانی (تا سوم خردادماه سال جاری) ، در اسرع وقت طبق دستورالعمل پیوست نسبت به ثبت نام اقدام فرمایید

https://meetings.unoda.org/section/oewg-ict-2021_ngo-information_16382
https://forms.office.com/pages/responsepage.aspx?id=2zWeD09UYE-9zF6kFubccMjpoC_xkItNrRxNChY4OtFUN1BKSFNCWjcwTkVUNkxWQlFESTdGQ1BEWS4u

https://bit.ly/ICTOEWG22

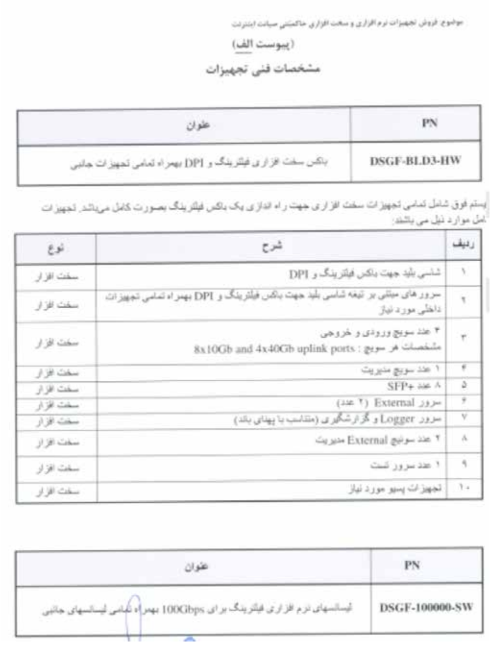
mail to prizeman@un.org

با تشکر
امیری

According to the documents obtained by Filterwatch, from 2006 to 2019, Douran Group had multiple contracts with various companies, including MCI (Hamrah Aval), Irancell, Telecommunications Infrastructure Company (TIC), Institute for Research in Fundamental Sciences (IPM), Rightel, and several other service providers. These contracts were worth 2,084,471,813,523 Rials. It's important to note that these figures do not cover all the contracts executed during that specific timeframe. A few of these contracts were denominated in US dollars. For instance, in 2019, there were two contracts valued at $901,018 each, and in 2018, another contract worth $3,456,000 was established.

Some of these contracts are as follows.

Contract No	Year	Contracting Party	Amount in Rials	USD Contract	License Type
1678	1396	MCI	25,668,000,000	-	80Gbps
1662	1396	MCI	12,834,000,000	-	40Gbps
5997	1399	Irancell	584,288,000,000	901,018	Selling security software and hardware equipment
9061/4996	1386	Irancell	99,161,000,000	-	-
4293	1397	Irancell	260,107,200,000	3,456,000	100Gbps
4224	1394	TIC	63,041,077,400	-	-
1678	1396	MCI		-	40G+40G
1126		Information technology company	8,878,915,556		The internal Internet blocking and censoring system of the first phase based on the tender 17/85
		Rightel	7,467,910,000	-	Buying lines and performing engineering services, integrating and upgrading the capacity of the Policy Enforcement system from 80 Gbps to 160 Gbps
7318	1390	IPM	69,000,000	-	128Mb/ps
19919	1396	TIC	1,701,300,000	-	Two firewall devices
8560	1396	TIC	501,067,895,917	-	Purchase of hardware upgrade equipment and development and software upgrade of international data traffic Internet blocking and censoring systems, phase 5
6578	1386	TIC	9,494,160,000	-	Internal Internet blocking and censoring of international data traffic
127736	1392	TIC	23,924,548,000	-	Phase one Internet blocking and censoring support services and additional equipment
201/584	1393	TIC	35,498,181,850	-	Buying Internet blocking and censoring server improvement equipment and providing software licenses
6213	1394	TIC	432,372,647,200	-	Purchase of Internet blocking and censoring traffic Internet blocking and censoring systems - Phase 4
96-95	1385	TIC	18,442,977,600	-	Separation of domestic and global traffic



موضوع: فروش تجهیزات نرم افزاری و سخت افزاری حاکمیتی صیانت اینترنت

(پیوست الف)

مشخصات فنی تجهیزات

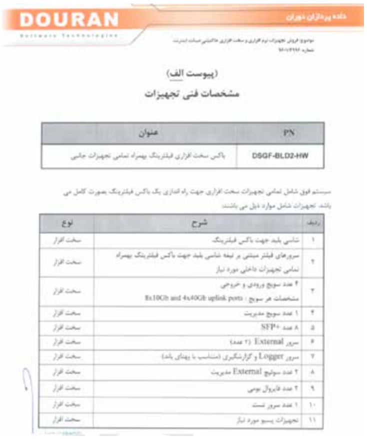
PN	عنوان
DSGF-BLD3-HW	باکس سخت افزاری فیلترینگ و DPI بهمراه تمامی تجهیزات جانبی

یستم فوق شامل تمامی تجهیزات سخت افزاری جهت راه اندازی یک باکس فیلترینگ بصورت کامل می‌باشد. تجهیزات
امل موارد ذیل می باشند:

ردیف	شرح	نوع
۱	شاسی بلید جهت باکس فیلترینگ و DPI	سخت افزار
۲	سرور های مبتنی بر تیغه شاسی بلید جهت باکس فیلترینگ و DPI بهمراه تمامی تجهیزات داخلی مورد نیاز	سخت افزار
۳	۴ عدد سویچ ورودی و خروجی مشخصات هر سویچ : 8x10Gb and 4x40Gb uplink ports	سخت افزار
۴	۱ عدد سویچ مدیریت	سخت افزار
۵	۸ عدد SFP+	سخت افزار
۶	سرور External (۲ عدد)	سخت افزار
۷	سرور Logger و گزارشگیری (متناسب با پهنای باند)	سخت افزار
۸	۲ عدد سوئیچ External مدیریت	سخت افزار
۹	۱ عدد سرور تست	سخت افزار
۱۰	تجهیزات پسیو مورد نیاز	سخت افزار

PN	عنوان
DSGF-100000-SW	لیسانسهای نرم افزاری فیلترینگ برای 100Gbps بهمراه تمامی لیسانسهای جانبی

Image of censorship services to Irancell under the title of protection



DOURAN
Software Technologies
داده پردازان دوران

موضوع: فروش تجهیزات نرم افزاری و سخت افزاری حاکمیتی صیانت اینترنت
شماره: [illegible]

(پیوست الف)

مشخصات فنی تجهیزات

PN	عنوان
DSGF-BLD2-HW	باکس سخت افزاری فیلترینگ بهمراه تمامی تجهیزات جانبی

سیستم فوق شامل تمامی تجهیزات سخت افزاری جهت راه اندازی یک باکس فیلترینگ بصورت کامل می باشد. تجهیزات شامل موارد ذیل می باشند:

ردیف	شرح	نوع
۱	شاسی بلید جهت باکس فیلترینگ	سخت افزار
۲	سرورهای فیلتر مبتنی بر تیغه شاسی بلید جهت باکس فیلترینگ بهمراه تمامی تجهیزات داخلی مورد نیاز	سخت افزار
۳	۴ عدد سویچ ورودی و خروجی مشخصات هر سویچ : 8x10Gb and 4x40Gb uplink ports	سخت افزار
۴	۱ عدد سویچ مدیریت	سخت افزار
۵	۸ عدد SFP+	سخت افزار
۶	سرور External (۲ عدد)	سخت افزار
۷	سرور Logger و گزارشگیری (متناسب با پهنای باند)	سخت افزار
۸	۲ عدد سوئیچ External مدیریت	سخت افزار
۹	۲ عدد فایروال بومی	سخت افزار
۱۰	۱ عدد سرور تست	سخت افزار
۱۱	تجهیزات پسیو مورد نیاز	سخت افزار

Image of censorship technical services to Irancell under the title of protection

Among the contracts primarily focused on the development of Internet blocking and censoring systems, two contracts stand out.

- A contract between Douran and Irancell in 2018 for technical services related to Internet blocking and censoring under the title of “protection.”

- A contract between Douran and TCI in 2016 for the amount of 600,442,977,18 Rials. It involved the purchase of hardware and software equipment, as well as implementation services, to establish infrastructure for separating domestic traffic from global

> traffic in several regions of the telecommunication company. The regions included Khorasan Razavi, Hamedan, Ilam, South Khorasan, Chaharmahal and Bakhtiari, Kerman, Khuzestan, Kurdistan, Sistan and Baluchistan, Golestan, Gilan, and North Khorasan provinces.

The policy of traffic separation was initially introduced during Hassan Rouhani's government. This policy enabled the Iranian government to facilitate easier censorship and disruption of the international Internet. This also allowed the government to disconnect the global Internet while minimizing any adverse impact of the internal systems of the Islamic Republic.

Since 2018, the Islamic Republic of Iran has disconnected the global Internet on ten occasions. These disconnections have consistently occurred in response to street demonstrations, during which numerous Iranian citizens were injured, imprisoned or killed. In this context, companies like Douran play a significant role in not only facilitating Internet censorship but also contributing to the suppression of protesters in the streets.

Islamic Revolutionary Guard Corps: Network Encryption Contract

A contract was signed between Douran and Amir Tavakoli, representing the Islamic Revolutionary Guard Corps, on 11/12/1394. The contract pertains to the purchase, support, and training of 100 network encryption hardware devices manufactured by Douran. The total value of this contract amounts to 1 billion Rials.

Blocking Circumvention Tools and VPNs

In a letter sent by Mehdi Amiri of the Attorney General's Office in 2017 to Douran company, they were invited to a meeting with the purpose of "examining the actions and operation of that company in the field of content blocking and censoring and countering of non-filter breakers and VPNs."

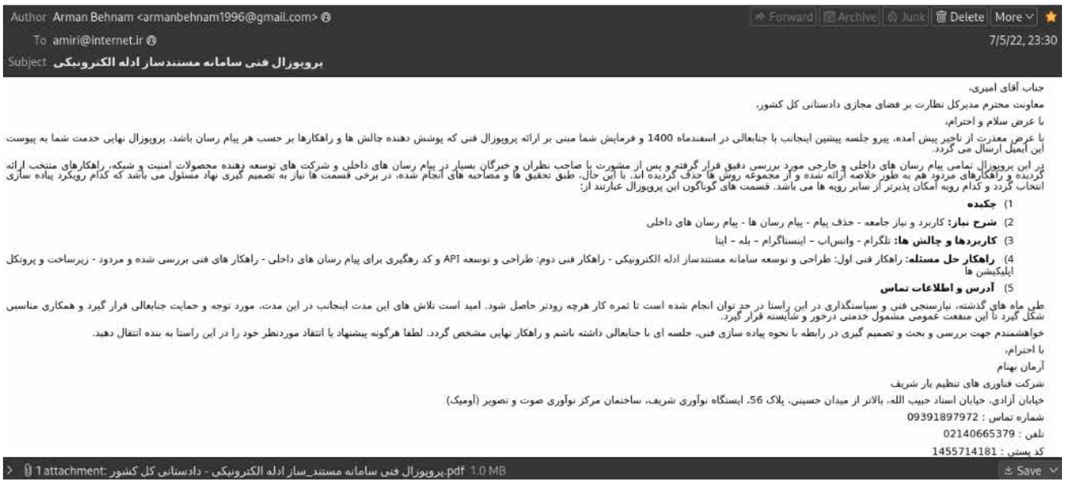
In the text of the letter, there is a conversation about the mission that was given to this company and further clarification about its role: "In the implementation of the mission assigned by the honorable Attorney General's Office to this investigation team, it is necessary to investigate its actions and functioning. The company in the field of content Internet blocking and censoring and disabling unauthorized VPNs and filter breakers orders the informed and authorized representatives of that company to attend the following meeting on 06/13/97 at 10:00 AM to 11:00 AM at the General Attorney General's Office of the country."

The letter was addressed to Reza Taqipour, who served as the head of the investigation board of the Attorney General's Office at the time. It is worth noting that Reza Taghipour, who received this letter, later went on to become a member of the Supreme Council of Cyberspace.

Tanzim-yar Sharif Technology

Tanzim-yar Sharif Technology is a company launched by Rasul Jalili, the president of Sharif University and member of the Supreme Council of CyberSpace. The main objective of this company is to support research and development efforts related to the tools required by the Attorney General's Office.

On July 5, 2022, Tanzimyar Sharif Technology sent a PDF file with the title "Technical proposal for the electronic evidence documenting system" to the technical director of the deputy director of cyberspace affairs of the Attorney General's Office. The document outlined "Adalat Yar," a platform designed for collecting, accessing, and presenting authentic electronic evidence in court proceedings. This document provides new insights regarding the tools employed by the Attorney General's Office for gathering evidence against individuals rather than institutions and companies.



Author Arman Behnam <armanbehnam1996@gmail.com>
To amiri@internet.ir
Subject پروپوزال فنی سامانه مستندساز ادله الکترونیکی
7/5/22, 23:30

جناب آقای امیری،
معاونت محترم مدیرکل نظارت بر فضای مجازی دادستانی کل کشور،
با عرض سلام و احترام،

با عرض معذرت از تاخیر پیش آمده، پیرو جلسه پیشین اینجانب با جنابعالی در اسفندماه 1400 و فرمایش شما مبنی بر ارائه پروپوزال فنی که پوشش دهنده چالش ها و راهکارها بر حسب هر پیام رسان باشد، پروپوزال نهایی حدمت شما به پیوست این ایمیل ارسال می گردد.

در این پروپوزال تمامی پیام رسان های داخلی و خارجی مورد بررسی دقیق قرار گرفتم و پس از مشورت با صاحب نظران و خبرگان بسیار در پیام رسان های داخلی و شرکت های توسعه دهنده محصولات امنیت و شبکه، راهکارهای منتخب ارائه گردیده و راهکارهای مردود هم به طور خلاصه ارائه شده و از مجموعه روش ها حذف گردیده اند. با این حال، طبق تحقیق ها و مصاحبه های انجام شده، در برخی قسمت ها نیاز به تصمیم گیری نهاد مسئول می باشد که کدام رویکرد پیاده سازی انتخاب گردد و کدام رویه امکان پذیرتر از سایر رویه ها می باشد. قسمت های گوناگون این پروپوزال عبارتند از:

1) **چکیده**
2) **شرح نیاز:** کاربرد و نیاز جامعه - حذف پیام - پیام رسان ها - پیام رسان های داخلی
3) **کاربردها و چالش ها:** تلگرام - واتس‌اپ - اینستاگرام - بله - ایتا
4) **راهکار حل مسئله:** راهکار فنی اول: طراحی و توسعه سامانه مستندساز ادله الکترونیکی - راهکار فنی دوم: طراحی و توسعه API و کد رهگیری برای پیام رسان های داخلی - راهکار های فنی بررسی شده و مردود - زیرساخت و پروتکل اپلیکیشن ها
5) **آدرس و اطلاعات تماس**

طی ماه های گذشته، نیازسنجی فنی و سیاستگذاری در این راستا در حد توان انجام شده است تا ثمره کار هرچه زودتر حاصل شود. امید است تلاش های این مدت اینجانب در این مدت، مورد توجه و حمایت جنابعالی قرار گیرد و همکاری مناسبی شکل گیرد تا این منفعت عمومی مشمول خدمتی درخور و شایسته قرار گیرد.

خواهشمندم جهت بررسی و بحث و تصمیم گیری در رابطه با نحوه پیاده سازی فنی، جلسه ای با جنابعالی داشته باشم و راهکار نهایی مشخص گردد. لطفا هرگونه پیشنهاد یا انتقاد موردنظر خود را در این راستا به بنده انتقال دهید.

با احترام،
آرمان بهنام
شرکت فناوری های تنظیم یار شریف
خیابان آزادی، خیابان استاد حبیب الله، بالاتر از میدان حسینی، پلاک 56، ایستگاه نوآوری شریف، ساختمان مرکز نوآوری صوت و تصویر (آومیک)
شماره تماس : 09391897972
تلفن : 02140665379
کد پستی : 1455714181

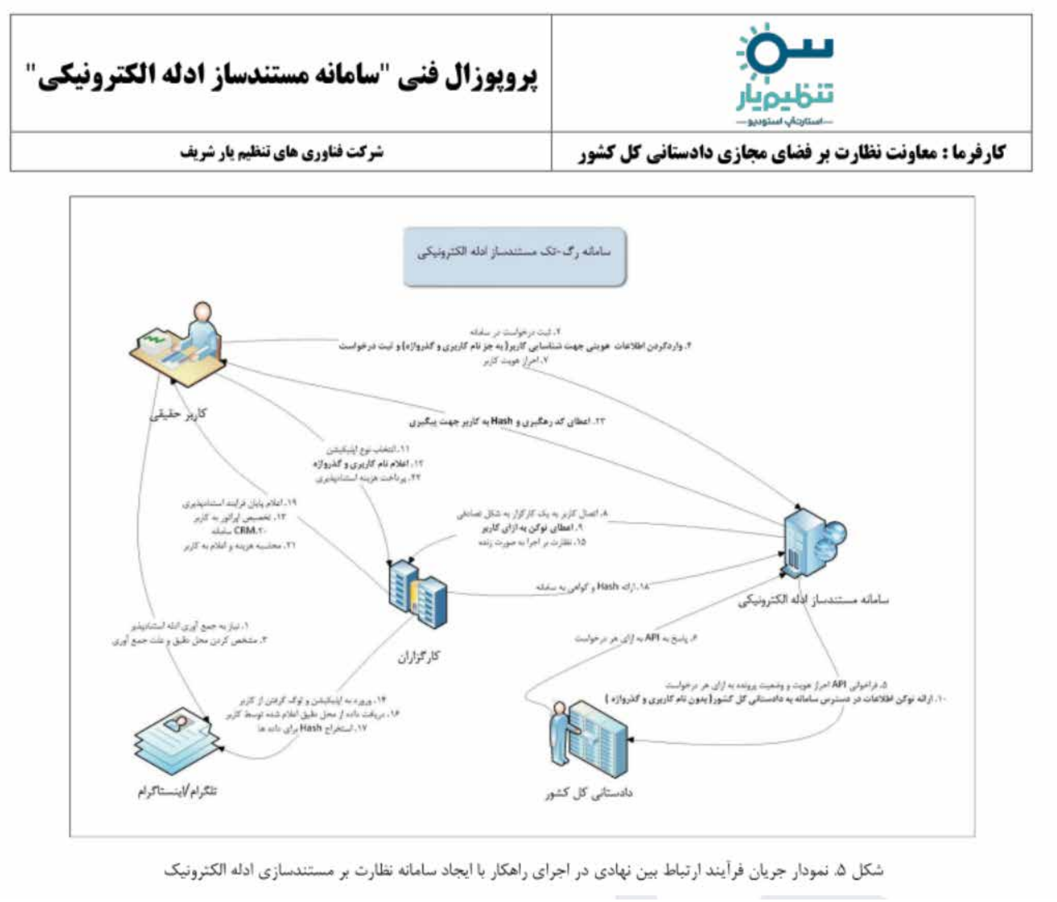
1 attachment: پروپوزال فنی سامانه مستند_ساز ادله الکترونیکی - دادستانی کل کشور.pdf 1.0 MB

The document states that one of the requirements is, "screenshots of chats and posts, account information, publication of false information". It also states that "deleting the message, in many messengers, after sending the message, it is possible to delete what is for the sender and even for the receiver, which makes no trace of the conversation. It didn't remain." This suggests that their solution for collecting information is taking screenshots so that even if a user enabled auto-disappearing messages, the act of taking screenshots can be utilized as a tool for data collection by preserving the content of those messages.

The document also states that "the courts, judicial authorities and FATA police[cyber police] do not have access to these data despite the many facilities to inquire about people's information. The existence of this system and the availability of its application for the people has made it possible for people to quickly collect electronic evidence and solve many problems and solve their concerns."

The approach implemented by Tanzimyar Shari Technologies for accessing the content of chats and emails of target groups involves the utilization of a third-party application. They say in this regard, "Adalat Yar's documenting system plan is implemented using the third-party concept with the aim of building trust between people and cyberspace and facilitating the process of hearing cases in the form of reg-tech technology."

Third-party applications are applications that are developed using legitimate APIs and obtain access to account information by acquiring permission from the respective account owners. A third-party app refers to an application



پروپوزال فنی "سامانه مستندساز ادله الکترونیکی"	تنظیم‌یار —استارتاپ استودیو—
شرکت فناوری های تنظیم یار شریف	کارفرما : معاونت نظارت بر فضای مجازی دادستانی کل کشور

سامانه رگ-تک مستندساز ادله الکترونیکی
کاربر حقیقی
۲. ثبت درخواست در سامانه
۴. واردکردن اطلاعات هویتی جهت شناسایی کاربر(به جز نام کاربری و گذرواژه) و ثبت درخواست
۷. احراز هویت کاربر
۲۳. اعطای کد رهگیری و Hash به کاربر جهت پیگیری
۱۱. انتخاب نوع اپلیکیشن
۱۲. اعلام نام کاربری و گذرواژه
۲۲. پرداخت هزینه استنادپذیری
۱۹. اعلام پایان فرایند استنادپذیری
۱۳. تخصیص اپراتور به کاربر
۲۰.CRM سامانه
۲۱. محاسبه هزینه و اعلام به کاربر
۸. اتصال کاربر به یک کارگزار به شکل تصادفی
۹. اعطای توکن به ازای کاربر
۱۵. نظارت بر اجرا به صورت زنده
۱۸. ارائه Hash و گواهی به سامانه
سامانه مستندساز ادله الکترونیکی
۱. نیاز به جمع آوری ادله استنادپذیر
۳. مشخص کردن محل دقیق و علت جمع آوری
کارگزاران
۶. پاسخ به API به ازای هر درخواست
۵. فراخوانی API احراز هویت و وضعیت پرونده به ازای هر درخواست
۱۰. ارائه توکن اطلاعات در دسترس سامانه به دادستانی کل کشور(بدون نام کاربری و گذرواژه)
۱۴. ورود به اپلیکیشن و توکن گرفتن از کاربر
۱۶. دریافت داده از محل دقیق اعلام شده توسط کاربر
۱۷. استخراج Hash برای داده ها
تلگرام/اینستاگرام
دادستانی کل کشور

شکل ۵. نمودار جریان فرآیند ارتباط بین نهادی در اجرای راهکار با ایجاد سامانه نظارت بر مستندسازی ادله الکترونیک

developed by a developer who is not the manufacturer of the device or the owner of the platform or website. Any developer can use the API provided by companies like Google or Telegram to create third-party apps. When running such applications, users are asked to grant permissions by the app. Unfortunately, due to lack of experience or knowledge, users may sometimes fall into traps and unintentionally grant excessive permissions to these apps, potentially compromising their privacy and security.

The document states, "In addition to the mentioned web contents, there are also social network contents. This content includes chat between two people, group chat and content of Telegram channels, content of Instagram posts, image and video content in the gallery and content of text messages, which in addition to the solutions mentioned, requires access to installation programs and running programs of the system. By checking them, it detects fake applications and fake screenshots from the source."

Regarding the production cost of this system, the final price is estimated at 250 million Tomans. The document states, "The finished price of the product is equivalent to 250 million Tomans for research and development, 360 million Tomans for construction and implementation and tests, and 190 million Tomans for creating promotional products and introducing, documenting and training this system. The total cost of developing this product is 800 million tomans."

The names and details of those who work on this system are mentioned as follows:

Name	Education	University	Field of Study	Role in the project
Arman Behnam	Master	Iran University of Science and Technology - Faculty of Industrial Engineering	Industrial Engineering	Project definition - idea generation - market studies - project management - process definition - description of the solution and its structure
Mahmoud Aghvami Panah	PhD	University of Tehran	Computer Engineering	System development manager
Kamil Shah Hosseini	PhD	University of Science and Industry	Computer Engineering	Developer

One of the methods used by government hackers is to create third-party applications that can access user accounts and collect information from them.

Lifeweb Social Network Analysis

On January 15, 2020, LifeWeb conducted a detailed analysis of Iranian users' reactions on Twitter, Instagram, and Telegram regarding the Ukrainian plane tragedy. The findings of this analysis were provided to the Attorney General's Office. Part of LifeWeb's analysis states, "Based on sentiment analysis of Persian posts on Twitter, the negative human emotions on this social media surpassed the anger and discontent over the November 2019 gasoline protests."

The report significantly refers to "incitement to protest and gathering (Amirkabir University and Azadi Square)." Bahareh Hedayat, a well-known civil rights activist, was arrested during this gathering and sentenced to eight months in prison on July 25, 2020, on charges of propaganda against the state, for tweeting.

LifeWeb goes beyond social network analysis and engages in political content analysis. This includes detailed analysis of statements made by Islamic Republic officials.

In another section of this report, it is stated about officials' statements after the U.S. killing of IRGC General Qassem Soleimani, "Two government figures, namely the Minister of Culture and Islamic Guidance and the President's Advisor, made separate attempts on Twitter to acknowledge the Commander's speech as necessary but insufficient. Other government figures did not delve much into the matter, and the Foreign Minister contented himself with posting a black image symbolizing mourning. However, two reformist factions, one political - Shahindokht Mowlaverdi, Mahmoud Sadeghi, etc. - and the other social - Abbas Abdi, Mohammad Fazeli, Mohammad Reza Jalaeipour, etc. - also addressed the same subjects of 'public trust' and 'social' collapse."

It added, "Reformists, even regarding the funeral of martyred General Qassem Soleimani, who was a symbol and manifestation of social unity and harsh revenge against America, made efforts to forward the same old messages, namely the introduction of polarizing interpretations, such as what they call 'opposition to war,' and to negatively influence society. However, the unfortunate death of 60 compatriots in the funeral ceremony in Kerman, helped them greatly."

Tiered Internet

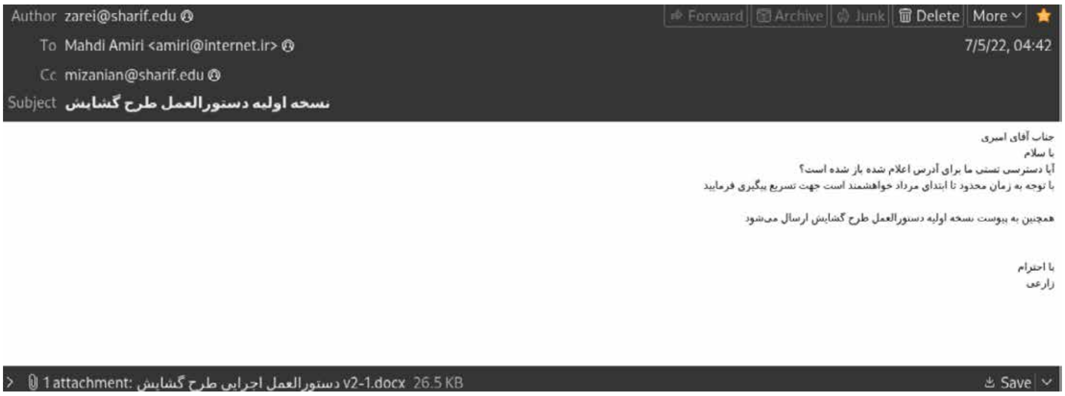
"Tiered Internet access" refers to a strategy that aims to reduce reliance on censorship and instead manage international bandwidth. The strategy involves providing different levels of Internet access to different groups of people based on their needs and roles.

The proposal for a tiered Internet system was first brought forward by Mohammad Javad Azari Jahormi, the Minister of Telecommunications during the second term of the Hassan Rouhani presidency (2013-2021). Jahromi highlighted the challenge posed by circumvention tools and emphasized the need for a plan to address this issue. He said, "Without organizing some areas, the issue of circumvention tools cannot be investigated. We said many times in different meetings to categorize [the accesses]. The level of the system for a doctor, for a university professor or for a journalist cannot be equal to the level of an eight or nine-year-old child."

Sharif's Goshayes plan; Initial test of tiered Internet

In a letter sent on July 5, 2022, an individual named Zarei from Sharif University addressed the Attorney General's Office, stating that "According to the permit number 140/1401/22812/9000 issued on June 20, 2022, the secretariat of the working group to determine instances of criminal content of the Attorney General's Office on a trial basis and for one year from July 23, 2033 in Sharif University of Technology in order to provide the possibility of access to clean resources for the selected community in a specific physical or virtual space in compliance with legal requirements and within the framework of specific laws and regulations."

Zarei, the sender of the letter, also complains about the delay in providing the requested access.



Author zarei@sharif.edu
To Mahdi Amiri <amiri@internet.ir>
Cc mizanian@sharif.edu
Subject نسخه اولیه دستورالعمل طرح گشایش
7/5/22, 04:42

جناب آقای امیری
با سلام
آیا دسترسی تستی ما برای آدرس اعلام شده باز شده است؟
با توجه به زمان محدود تا ابتدای مرداد خواهشمند است جهت تسریع پیگیری فرمایید

همچنین به پیوست نسخه اولیه دستورالعمل طرح گشایش ارسال می‌شود

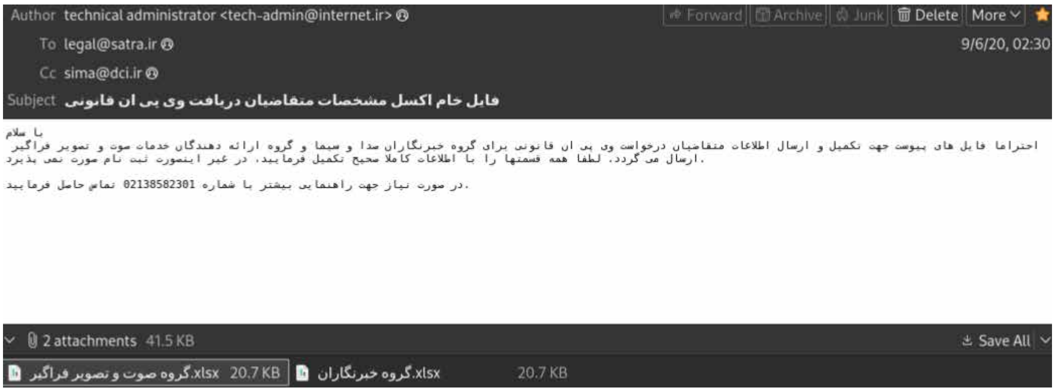
با احترام
زارعی

1 attachment: دستورالعمل اجرایی طرح گشایش v2-1.docx 26.5 KB

This request is related to providing uncensored Internet access for a group of people in Sharif University, which was supposed to be implemented on a trial basis. This service can be seen as an initial step towards establishing a tiered Internet system. To facilitate the implementation of this service, a range of IP addresses associated with the university has been whitelisted.

Legal VPN

An email sent to SATRA about a year ago revealed that in the past, tiered Internet access was provided through the use of legal VPNs. The email, dated September 17, 2019, was from the Technical Director of the Attorney General's Office and contained two Excel files for applicants who wished to obtain a legal VPN.



Author technical administrator <tech-admin@internet.ir>
To legal@satra.ir
Cc sima@dci.ir
9/6/20, 02:30
Subject فایل خام اکسل مشخصات متقاضیان دریافت وی پی ان قانونی

با سلام
احتراما فایل های پیوست جهت تکمیل و ارسال اطلاعات متقاضیان درخواست وی پی ان قانونی برای گروه خبرنگاران صدا و سیما و گروه ارائه دهندگان خدمات صوت و تصویر فراگیر
ارسال می گردد. لطفا همه قسمتها را با اطلاعات کاملا صحیح تکمیل فرمایید. در غیر اینصورت ثبت نام صورت نمی پذیرد

در صورت نیاز جهت راهنمایی بیشتر با شماره 02138582301 تماس حاصل فرمایید.

2 attachments 41.5 KB
گروه صوت و تصویر فراگیر.xlsx 20.7 KB
گروه خبرنگاران.xlsx 20.7 KB

This plan was first introduced as a "Legal VPN" in response to the challenges associated with the Internet shutdown during the bloody November 2019 protests. It aimed to establish a framework for tiered Internet access.

While the tiered Internet connection in Sharif University was implemented using the whitelist method, this email shows that legal VPNs were also used for providing different levels of Internet access.

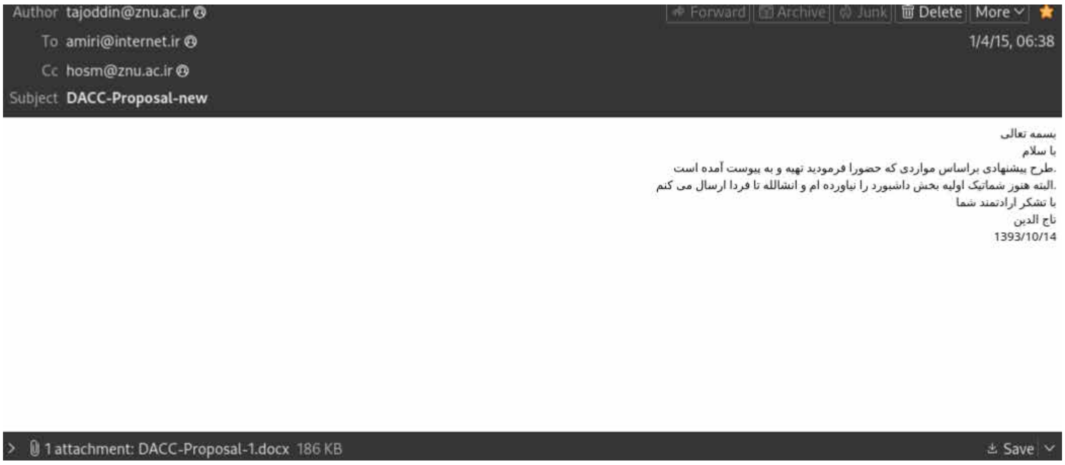
Legal and Technical Research

Much of the content of the Attorney General's Office's emails is related to legal and technical research concerning the restriction of Internet access or the criminalization of Internet activity.

Censorship Proposal

On December 14, 2014, Asghar Tajuddin, an assistant professor at Zanjan University, sent an email from his university email address (tajoddin@zan.au.ir, archived link) to the Attorney General's Office. In the email, he referenced suggestions that had been discussed during a previous face-to-face meeting.

This email, titled, "Content access management plan in the country," contained Mr. Tajuddin's technical proposals for Internet blocking and censoring, which were submitted to the Attorney General's Office. According to the information in this file, this plan "belongs to Sana Sharq System Development Company."



Author tajoddin@znu.ac.ir
To amiri@internet.ir
Cc hosm@znu.ac.ir
Subject DACC-Proposal-new
1/4/15, 06:38

بسمه تعالی
با سلام
.طرح پیشنهادی براساس مواردی که حضورا فرمودید تهیه و به پیوست آمده است
.البته هنوز شماتیک اولیه بحش داشبورد را نیاورده ام و انشالله تا فردا ارسال می کنم
با تشکر ارادتمند شما
تاج الدین
1393/10/14

1 attachment: DACC-Proposal-1.docx 186 KB

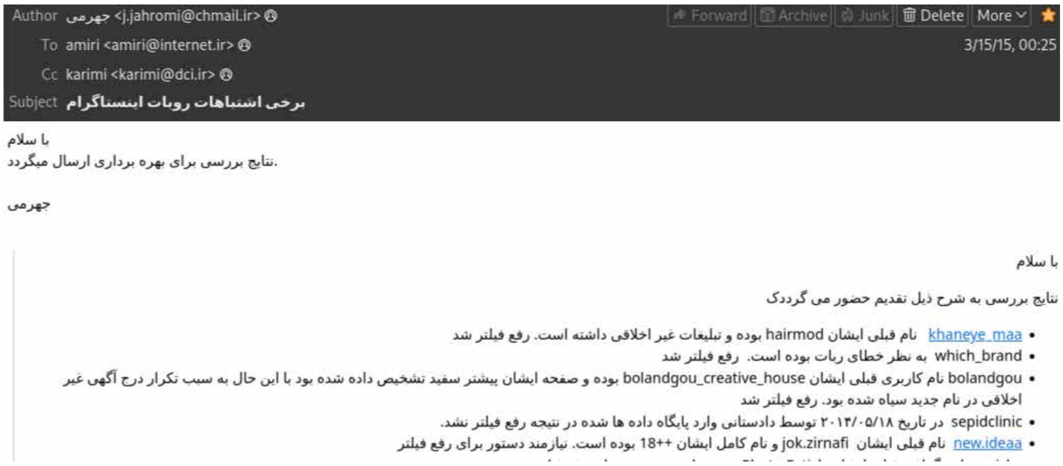
تصویر ایمیل اصغر تاج‌الدین به دادستانی به همراه فایل پروپوزال طرح فیلترینگ

Instagram Bot

On February 25, 2014, Mohammad Javad Azari Jahormi sent an email to the Attorney General's Office presenting a report on the performance of the Instagram-post-recognition machine.

It seems that when the Instagram-post-recognition machine was operational, Instagram did not encrypt connections using the SSL/TLS protocol yet. This allowed the Iranian government to censor Instagram pages.

This project involving the Instagram-post-recognition machine continued until 2017. This is evidenced by a letter sent on November 19, 2017 from



Author جهرمی <j.jahromi@chmail.ir>
To amiri <amiri@internet.ir>
Cc karimi <karimi@dci.ir>
Subject برخی اشتباهات روبات اینستاگرام
3/15/15, 00:25

با سلام
.نتایج بررسی برای بهره برداری ارسال میگردد

جهرمی

با سلام

نتایج بررسی به شرح ذیل تقدیم حضور می گرددک

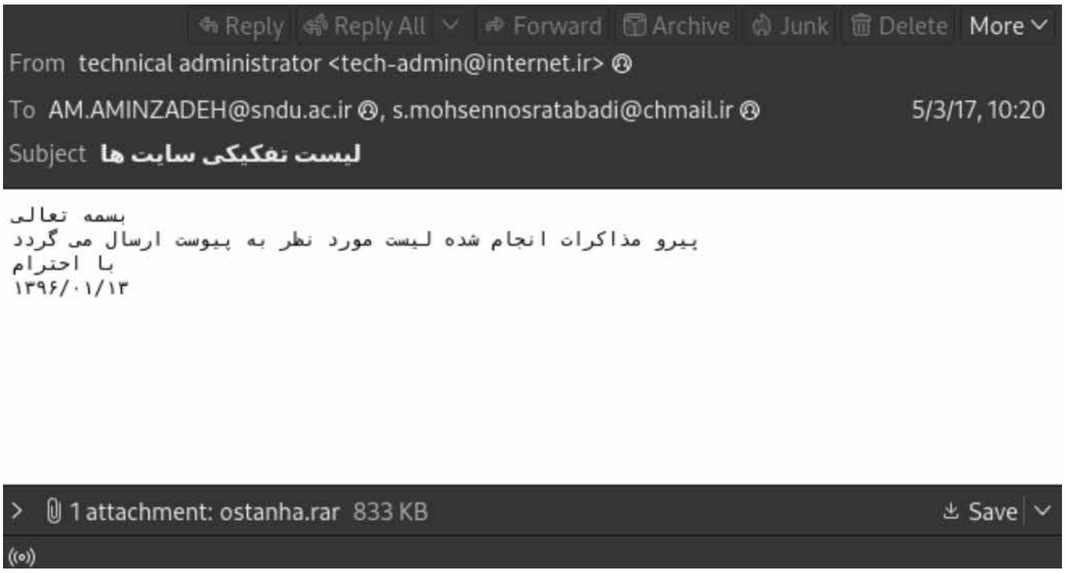
- khaneye_maa نام قبلی ایشان hairmod بوده و تبلیغات غیر اخلاقی داشته است. رفع فیلتر شد
- which_brand به نظر خطای ربات بوده است. رفع فیلتر شد
- bolandgou نام کاربری قبلی ایشان bolandgou_creative_house بوده و صفحه ایشان پیشتر سفید تشخیص داده شده بود با این حال به سبب تکرار درج آگهی غیر اخلاقی در نام جدید سیاه شده بود. رفع فیلتر شد
- sepidclinic در تاریخ ۲۰۱۴/۰۵/۱۸ توسط دادستانی وارد پایگاه داده ها شده در نتیجه رفع فیلتر نشد.
- new.ideaa نام قبلی ایشان jok.zirnafi و نام کامل ایشان ++18 بوده است. نیازمند دستور برای رفع فیلتر

Javad Javidnia, the deputy head of cyberspace affairs of the Attorney General's Office, to Rasul Jalili. The letter communicated a meeting "regarding smart Internet blocking and censoring plans and how to deal with Instagram, in the presence of the representatives of this Attorney General's Office, the General Staff of the Armed Forces, the Intelligence Organization of the Revolutionary Guards and some other individuals members of the Supreme Council of CyberSpace."

We believe this was the time that smart Internet blocking and censoring was not useful anymore due to the implementation of SSL/TLS connections on Instagram.

Supreme National Defense University

The email address AM.AMINZADEH@sndu.ac.ir, belonging to the Supreme National Defense University (SNDU), emerged during the examination of the email exchanges related to the Chapar domestic search engine. This email belongs to Mohammad Ali Aminzadeh, a PhD student in strategic cyber studies at SNDU, who has published articles in the Journal of National Security.



From technical administrator <tech-admin@internet.ir>

To AM.AMINZADEH@sndu.ac.ir, s.mohsennosratabadi@chmail.ir 5/3/17, 10:20

Subject لیست تفکیکی سایت ها

بسمه تعالی
پیرو مذاکرات انجام شده لیست مورد نظر به پیوست ارسال می گردد
با احترام
۱۳۹۶/۰۱/۱۳

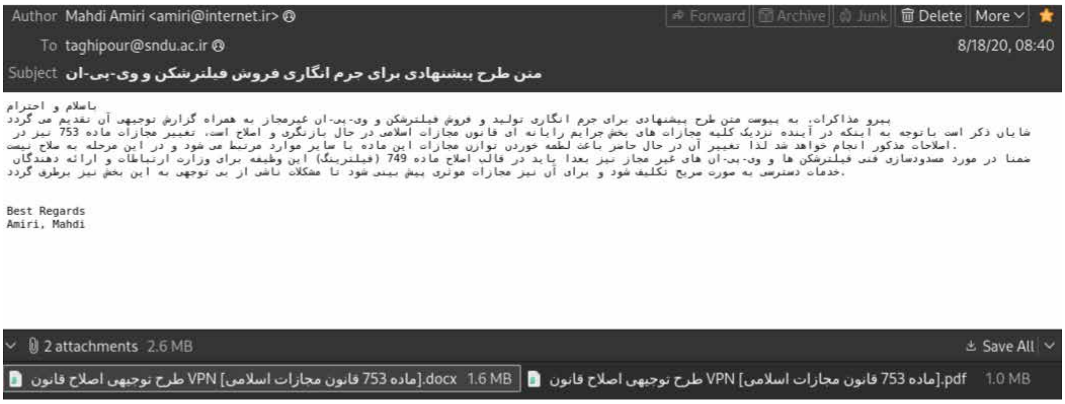
1 attachment: ostanha.rar 833 KB

One of Aminzadeh's recent articles is titled "Economic Opportunities and Threats Facing the Islamic Republic of Iran from the Cyber Technology Development in the Next Decade" (archived link) co-authored by Rasoul Ramezani, the Deputy in Charge of Research at the Khattam Al-Anbiya Air Defense University in Tehran, and assistant professor at Imam Hossein University.

SNDU is one of the universities affiliated with the armed forces of the Islamic Republic. The university was established in 1992 as the University of Strategic Sciences and became a subsidiary of the Armed Forces General Staff in 2002.

The presence of an email associated with the SNDU and its student related to the Chapar search engine suggests a collaboration between the armed forces and such national security projects. Notably, one of the main objectives of the online users protection bill was the transfer of control over the Internet in Iran to the armed forces, effectively leading to the militarization of online content.

On August 28, 2019, a plan to criminalize the sale of circumvention tools was sent from the Attorney General's Office to Reza Taghipour Anwari (taghipour@sndu.ac.ir) from SNDU. It was mentioned that sending this plan was based on "previous negotiations," indicating a close collaboration between the Attorney General's Office and SNDU on criminalizing the sale of circumvention tools. The exact role of military universities, such as SNDU, in the development of this bill is not clear. However, it can be inferred that these universities at least have an advisory role in the design of such a bill.



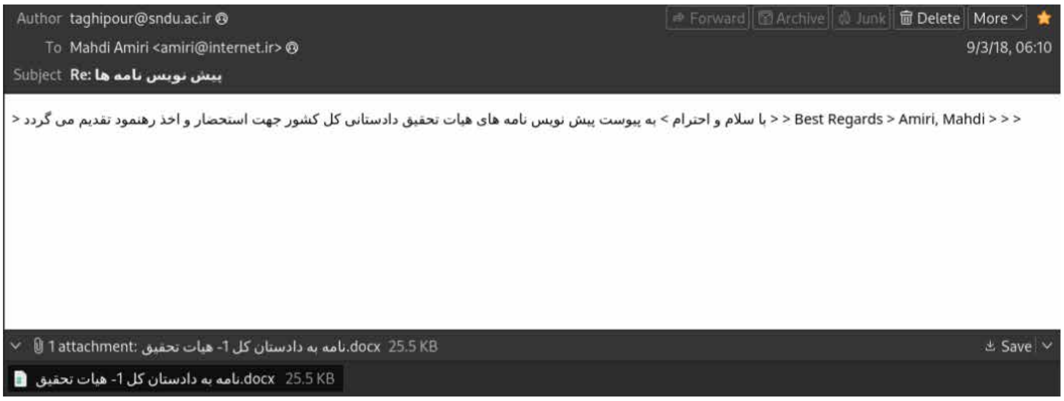
Author Mahdi Amiri <amiri@internet.ir>
To taghipour@sndu.ac.ir
8/18/20, 08:40
Subject متن طرح پیشنهادی برای جرم انگاری فروش فیلترشکن و وی-پی-ان

باسلام و احترام
پیرو مذاکرات، به پیوست متن طرح پیشنهادی برای جرم انگاری تولید و فروش فیلترشکن و وی-پی-ان غیرمجاز به همراه گزارش توجیهی آن تقدیم می گردد
شایان ذکر است باتوجه به اینکه در آینده نزدیک کلیه مجازات های بخش جرایم رایانه ای قانون مجازات اسلامی در حال بازنگری و اصلاح است، تغییر مجازات ماده 753 نیز در
اصلاحات مذکور انجام خواهد شد لذا تغییر آن در حال حاضر باعث لطمه خوردن توازن مجازات این ماده با سایر موارد مرتبط می شود و در این مرحله به صلاح نیست.
ضمنا در مورد مسدودسازی فنی فیلترشکن ها و وی-پی-ان های غیر مجاز نیز بعدا باید در قالب اصلاح ماده 749 (فیلترینگ) این وظیفه برای وزارت ارتباطات و ارائه دهندگان
خدمات دسترسی به صورت صریح تکلیف شود و برای آن نیز مجازات موثری پیش بینی شود تا مشکلات ناشی از بی توجهی به این بخش نیز برطرف گردد.

Best Regards
Amiri, Mahdi

2 attachments 2.6 MB
Save All
طرح توجیهی اصلاح قانون VPN [ماده 753 قانون مجازات اسلامی].docx 1.6 MB
طرح توجیهی اصلاح قانون VPN [ماده 753 قانون مجازات اسلامی].pdf 1.0 MB

In other email exchanges between the Attorney General's Office and Taghipour from SNDU, various plans regarding the National Information Network, blocking Telegram, and access to censorship data have been discussed.



Author taghipour@sndu.ac.ir
To Mahdi Amiri <amiri@internet.ir>
9/3/18, 06:10
Subject Re: پیش نویس نامه ها

> با سلام و احترام > به پیوست پیش نویس نامه های هیات تحقیق دادستانی کل کشور جهت استحضار و اخذ رهنمود تقدیم می گردد > > Best Regards > Amiri, Mahdi > > >

1 attachment: نامه به دادستان کل -1 هیات تحقیق.docx 25.5 KB
Save
نامه به دادستان کل -1 هیات تحقیق.docx 25.5 KB

In this email it is stated, "From the beginning of the mission, the necessary preliminary measures to access the required information and systems has carried out technical reviews and in-person inspections of the systems and centers of the Ministry of Telecommunications and Information Technology, but in order to access to the system an information required necessary permits by the relevant authorities in ministries of TIC and MOIS, yet the requested information has not been received to carry out the mentioned research."

In light of the challenges faced in accessing the required information and systems, Taghipour requested an extension of the mission duration. Furthermore, they specifically urged the Attorney General's office to issue an order to TIC to provide access to "the country's international traffic Internet blocking and censoring and analysis systems and information related to the traffic of foreign and domestic social messaging software and circumvention tools."

Legal Solutions for Organizing Virtual Space

A document discovered among the emails outlined several proposed legal solutions aimed at organizing cyberspace. These solutions were mainly focused on censorship and restricting access to the Internet and messaging applications. They included:

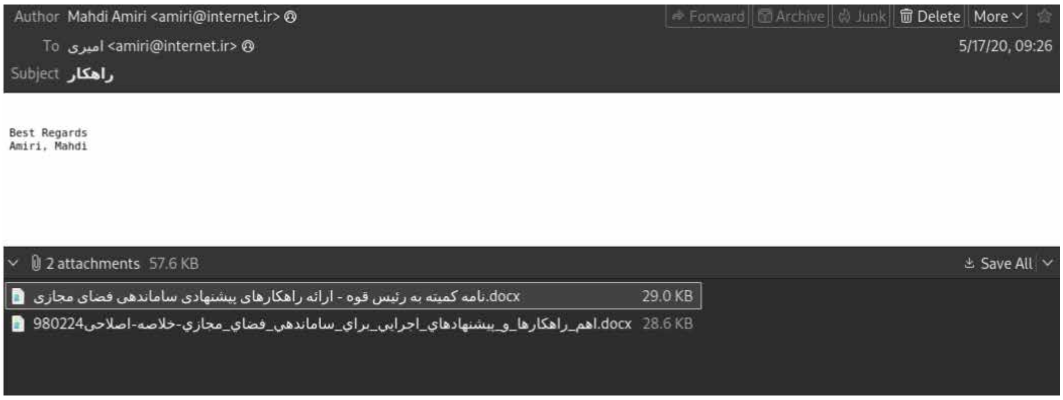
» Complete, effective and continuous blocking of all circumvention tools and unauthorized VPNs.

» Bandwidth reduction and gradual blocking of Google Play and foreign social messaging apps, especially Instagram and WhatsApp.

» Interrupting or effectively disrupting audio and video conversations (LiveStream) on Instagram and WhatsApp (The legal, technical and operational bases of these mechanisms are attached).

The document highlighted the significance and urgency of implementing these proposed measures by referencing meetings attended by key stakeholders, including the Attorney General of the country and the General Staff of the Armed Forces. Additionally, the document emphasized the written approvals received from Ayatollah Ali Khamenei, the Supreme Leader of Iran.

The document continued, "However, since the government has not been



Author Mahdi Amiri <amiri@internet.ir>
To امیری <amiri@internet.ir>
5/17/20, 09:26
Subject راهکار

Best Regards
Amiri, Mahdi

2 attachments 57.6 KB

نامه کمیته به رئیس قوه - ارائه راهکارهای پیشنهادی ساماندهی فضای مجازی.docx	29.0 KB
اهم_راهكارها_و_پيشنهادهاي_اجرايي_براي_ساماندهي_فضاي_مجازي-خلاصه-اصلاحی980224.docx	28.6 KB

willing to implement these resolutions and the judicial system has not had a serious determination to deal with violations, these measures and decisions have not been implemented in practice, so it is suggested to continuously follow up on the organization of cyberspace be done below."

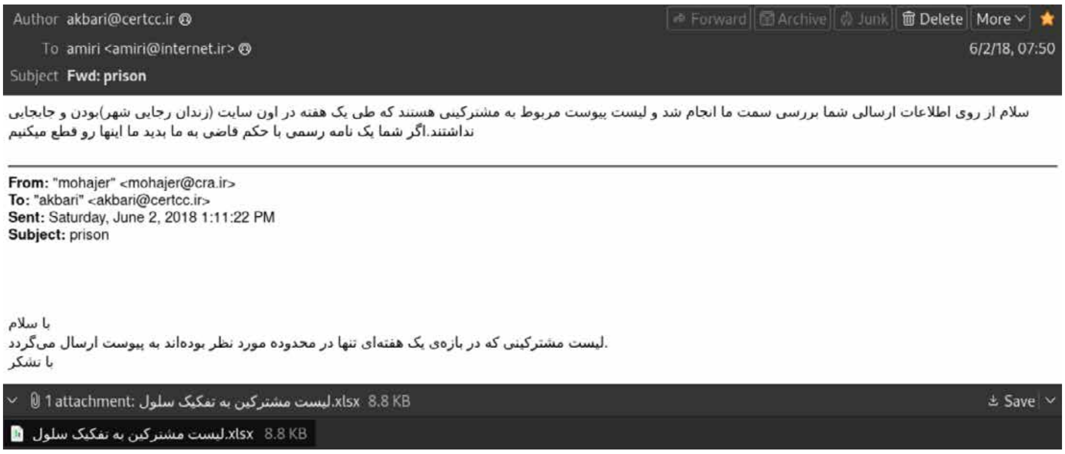
Based on the proposal, the document suggested the formation of a committee with representatives from the Attorney General's Office, the Information Technology Center of the Judiciary, the Intelligence Organization of the Revolutionary Guards, and two representatives from the Judiciary. The Attorney General's Office also recommended that the proposed methods be implemented through "online access to the network traffic control system and with the cooperation of law enforcement officers (preferably the IRGC)."

According to this document, detailed information about the country's network traffic status is "exclusively at the disposal of the General Directorate of Naja (Ministry of Intelligence) Network Security office." For this reason, the Attorney General's office has announced that this data is directly accessible with a judicial order or approval in the Supreme Council of CyberSpace.

Center of Iranian National Computer Emergency Response Team

Among the emails obtained from the Center of Iranian National Computer Emergency Response Team (CERT), also known as Maher Center, an email with the title "prison" draws attention.

In this email addressed to Amiri, it is written, "Hello, based on the information you sent, and investigation from our site, the attached list is the [mobile numbers of] subscribers who have not moved to that site (Rajai Shahr prison) within the past week. If you give us an official letter with the judge's order, we will cut them off."



Author akbari@certcc.ir
To amiri <amiri@internet.ir>
6/2/18, 07:50
Subject **Fwd: prison**

سلام از روی اطلاعات ارسالی شما بررسی سمت ما انجام شد و لیست پیوست مربوط به مشترکینی هستند که طی یک هفته در اون سایت (زندان رجایی شهر)بودن و جابجایی نداشتند.اگر شما یک نامه رسمی با حکم قاضی به ما بدید ما اینها رو قطع میکنیم

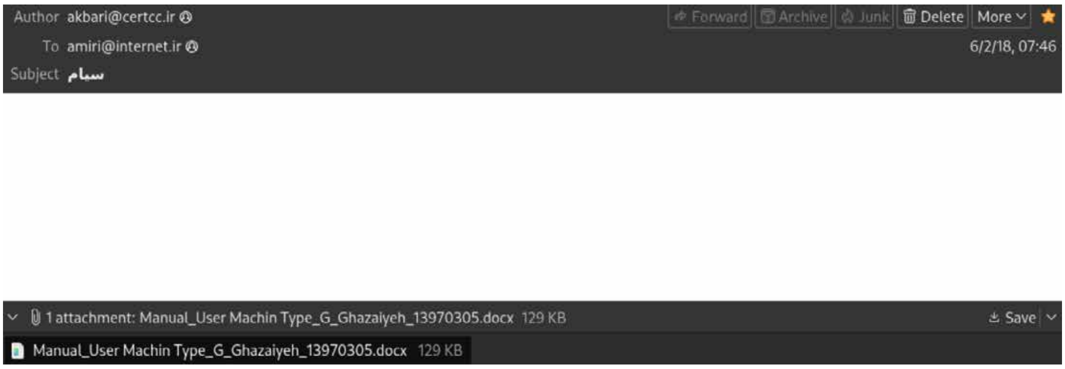
From: "mohajer" <mohajer@cra.ir>
To: "akbari" <akbari@certcc.ir>
Sent: Saturday, June 2, 2018 1:11:22 PM
Subject: prison

با سلام
لیست مشترکینی که در بازه‌ی یک هفته‌ای تنها در محدوده مورد نظر بوده‌اند به پیوست ارسال می‌گردد.
با تشکر

1 attachment: لیست مشترکین به تفکیک سلول.xlsx 8.8 KB
Save
لیست مشترکین به تفکیک سلول.xlsx 8.8 KB

This seems to be related to identifying inmates who were using cell phones in Rajai Shahr prison. In another email, the same person sends instructions to Mehdi Amiri in the Attorney General's office on how to use the SIAM system.

SIAM is a system developed by the Communications Regulatory Authority (CRA) and according to a report by The Intercept, this system provides the possibility of finding the geographic location of individuals based on their mobile number, geographical location, or IP address.



Author akbari@certcc.ir
To amiri@internet.ir
6/2/18, 07:46
Subject **سیام**

1 attachment: Manual_User Machin Type_G_Ghazaiyeh_13970305.docx 129 KB
Save
Manual_User Machin Type_G_Ghazaiyeh_13970305.docx 129 KB

The email also suggests that Maher is involved in the SIAM program.

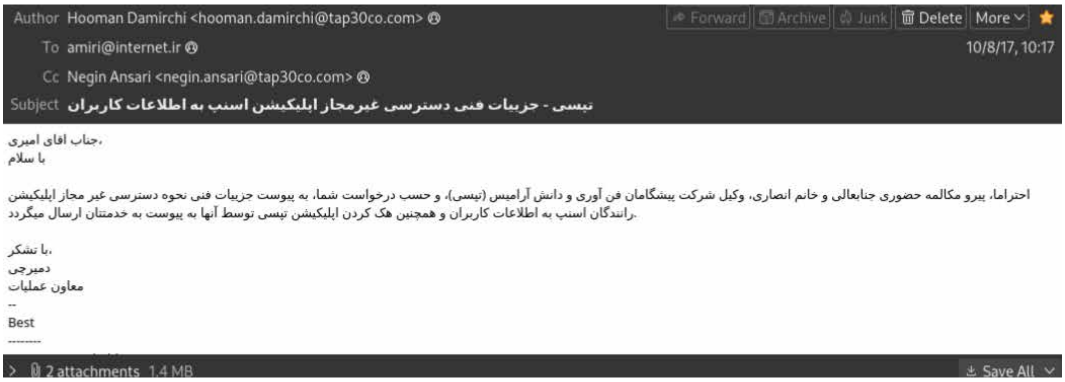
Applications

Most of the emails we reviewed focused on mobile apps.

Tapsi

In an email sent by Tapsi. An online taxi service, to the Attorney General's Office, Tapsi complains that the office does not prevent its competitor, Snap, from using Waze's live map.

In this email, a technical document is also attached, which technically proves that Snap uses Waze.



Author Hooman Damirchi <hooman.damirchi@tap30co.com>
To amiri@internet.ir
Cc Negin Ansari <negin.ansari@tap30co.com>
Subject تپسی - جزییات فنی دسترسی غیرمجاز اپلیکیشن اسنپ به اطلاعات کاربران
10/8/17, 10:17

جناب اقای امیری،
با سلام

احتراما، پیرو مکالمه حضوری جنابعالی و خانم انصاری، وکیل شرکت پیشگامان فن آوری و دانش آرامیس (تپسی)، و حسب درخواست شما، به پیوست جزییات فنی نحوه دسترسی غیر مجاز اپلیکیشن رانندگان اسنپ به اطلاعات کاربران و همچنین هک کردن اپلیکیشن تپسی توسط آنها به پیوست به خدمتتان ارسال میگردد.

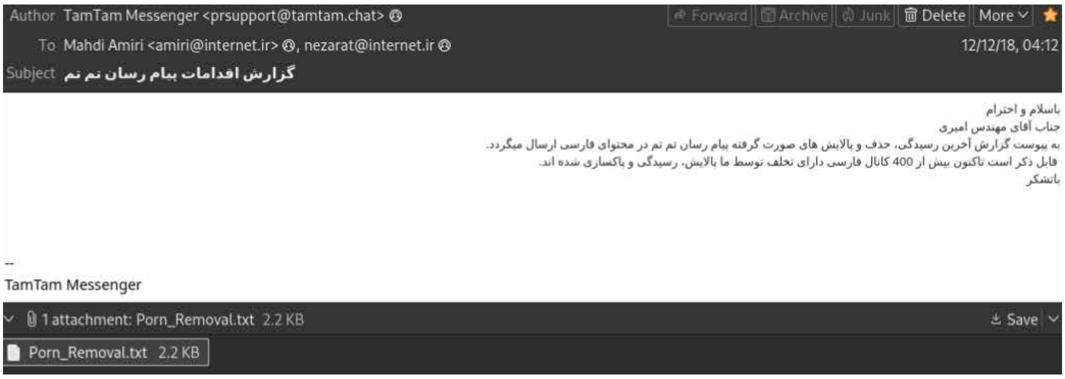
با تشکر،
دمیرچی
معاون عملیات
--
Best
----

2 attachments 1.4 MB

TamTam

In another email, the maker of the TemTem messaging application, which had gained popularity in Iran for a period, announced that it had removed content requested by the Attorney General's Office from its app.

It seems that these contents were pornographic, but this email shows that this company cooperated with the Iranian Attorney General's Office.



Author TamTam Messenger <prsupport@tamtam.chat>
To Mahdi Amiri <amiri@internet.ir>, nezarat@internet.ir
Subject گزارش اقدامات پیام رسان تم تم
12/12/18, 04:12

باسلام و احترام
جناب آقای مهندس امیری
به پیوست گزارش آخرین رسیدگی، حذف و پالایش های صورت گرفته پیام رسان تم تم در محتوای فارسی ارسال میگردد.
قابل ذکر است تاکنون بیش از 400 کانال فارسی دارای تخلف توسط ما پالایش، رسیدگی و پاکسازی شده اند.
باتشکر

--
TamTam Messenger

1 attachment: Porn_Removal.txt 2.2 KB
Porn_Removal.txt 2.2 KB

In another letter, a company called Hamamihan informs the Attorney General's Office that it is the official representative of this messenger in Iran. It says that it "considers itself obliged to carry out the necessary filtration on the Persian content, and for this reason, so far, from the side of this messenger, more than 400 channels and Persian content has been reviewed and filtration, and its list is attached."

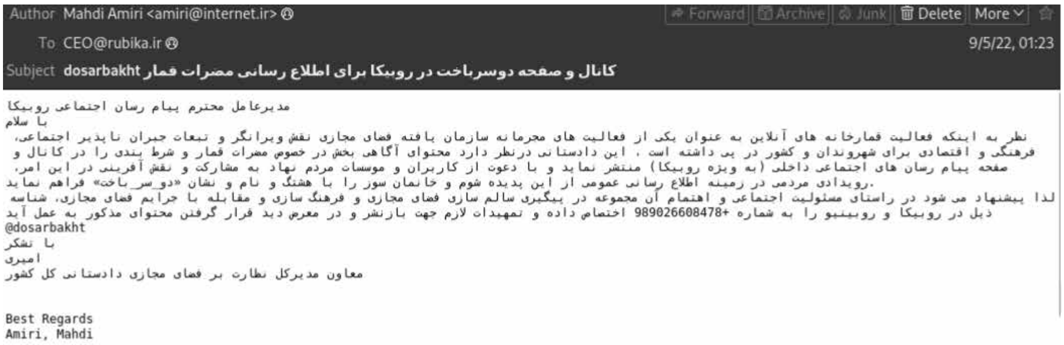
In the subsequent email, it is requested to remove the blocking of this messenger in Cafe Bazar, the domestic Android app store.

Rubika

Rubika is a domestic app created by the Tosca Company. According to official records, its major shareholders are: 'Mobile Telecommunications Company', 'Nagsh-e-Aval-e-Keyfiat' (NAK), (Persian: نقـش اول کیفیـت), and Noor Dana Development Capital, which are all subsidiaries of the TCI.
Forced Confession

One of the ways that the WGDICC targets individuals involved in gambling and financial transactions is by forcing them to record videos of themselves confessing and expressing regret for their actions. These videos are then posted on a specific channel on Rubika and Rubino applications, with the address (@dosarbakht) and a phone number, under the pretext of providing "informative content about the harms of gambling and betting."

This practice was revealed by an email dated May 9, 2022, from Mehdi Amiri, the Technical Director of the CyberSpace Affairs of the Attorney General's Office, to the director of Rubika. The email requested him to create the channel and post the videos on it.

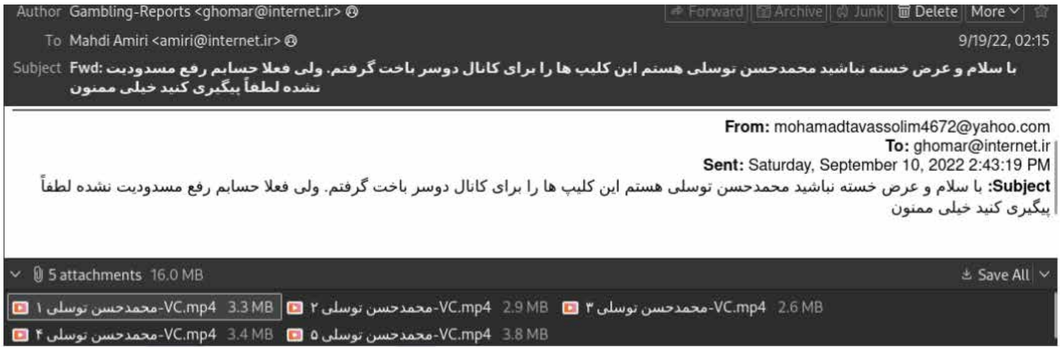


Author Mahdi Amiri <amiri@internet.ir>
To CEO@rubika.ir
9/5/22, 01:23
Subject dosarbakht کانال و صفحه دوسرباخت در روبیکا برای اطلاع رسانی مضرات قمار

```
مدیرعامل محترم پیام رسان اجتماعی روبیکا
با سلام
نظر به اینکه فعالیت قمارخانه های آنلاین به عنوان یکی از فعالیت های مجرمانه سازمان یافته فضای مجازی نقش ویرانگر و تبعات جبران ناپذیر اجتماعی،
فرهنگی و اقتصادی برای شهروندان و کشور در پی داشته است ، این دادستانی درنظر دارد محتوای آگاهی بخش در خصوص مضرات قمار و شرط بندی را در کانال و
صفحه پیام رسان های اجتماعی داخلی (به ویژه روبیکا) منتشر نماید و با دعوت از کاربران و موسسات مردم نهاد به مشارکت و نقش آفرینی در این امر،
رویدادی مردمی در زمینه اطلاع رسانی عمومی از این پدیده شوم و خانمان سوز را با هشتگ و نام و نشان «دو_سر_باخت» فراهم نماید.
لذا پیشنهاد می شود در راستای مسئولیت اجتماعی و اهتمام آن مجموعه در پیگیری سالم سازی فضای مجازی و فرهنگ سازی و مقابله با جرایم فضای مجازی، شناسه
ذیل در روبیکا و روبینو را به شماره 989026608478+ اختصاص داده و تمهیدات لازم جهت بازنشر و در معرض دید قرار گرفتن محتوای مذکور به عمل آید
@dosarbakht
با تشکر
امیری
معاون مدیرکل نظارت بر فضای مجازی دادستانی کل کشور


Best Regards
Amiri, Mahdi
```

Further investigations of Mr. Amiri's emails show that in order to unfreeze the bank accounts of individuals who are accused of gambling, the Attorney General's Office coerces them to take these videos and send them via email. For example, one of those who gambled on September 24, 2022 emailed several videos of his confession and regret, saying: "Greetings, don't be bored, [redacted] I took these clips for the Doser Bakht channel. But at the moment my account has not been unblocked, please follow up, thank you very much."

There are many examples of these types of emails in Mr. Amiri's inbox, and in some cases he even asks for modifications to the videos to address his concerns.



Author Gambling-Reports <ghomar@internet.ir>
To Mahdi Amiri <amiri@internet.ir>
9/19/22, 02:15
Subject Fwd: با سلام و عرض خسته نباشید محمدحسن توسلی هستم این کلیپ ها را برای کانال دوسر باخت گرفتم. ولی فعلا حسابم رفع مسدودیت نشده لطفاً پیگیری کنید خیلی ممنون

From: mohamadtavassolim4672@yahoo.com
To: ghomar@internet.ir
Sent: Saturday, September 10, 2022 2:43:19 PM
Subject: با سلام و عرض خسته نباشید محمدحسن توسلی هستم این کلیپ ها را برای کانال دوسر باخت گرفتم. ولی فعلا حسابم رفع مسدودیت نشده لطفاً پیگیری کنید خیلی ممنون

5 attachments 16.0 MB — Save All

محمدحسن توسلی ۱-VC.mp4 3.3 MB
محمدحسن توسلی ۲-VC.mp4 2.9 MB
محمدحسن توسلی ۳-VC.mp4 2.6 MB
محمدحسن توسلی ۴-VC.mp4 3.4 MB
محمدحسن توسلی ۵-VC.mp4 3.8 MB

These emails indicate that only individuals engaged in gambling activities were compelled to provide such videos and express regret. Surprisingly, we have not come across any evidence of actions taken against gambling companies or the individuals who operate these establishments.

Gambling

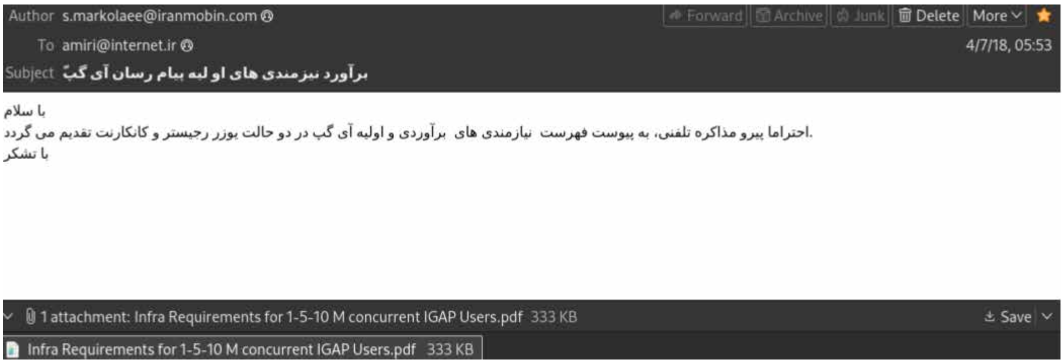
The WGDICC also collaborates with various companies and technologies to collect information on gambling and financial transactions. One of them is Kashef Secure Electronic Processing, which provides a web service specifically designed for this purpose. The WGDICC frequently requests customer identity information from banks, online payment gateways, and Fintech services without submitting an official request or a court-issued order. In almost all cases, these entities share the requested information and more via email.

Webamooz is a grassroots project specializing in financial cyber crimes that has documented most of the cases related to gambling, financial transactions, and similar matters mentioned in the WGDICC's emails.

Gap and iGap

In the email sent to the Attorney General's Office, the messenger application named iGap outlined its technical requirements, indicating an expectation for support.

In another email, Gap provided information about a group called "Duel Girls" to the Attorney General's Office

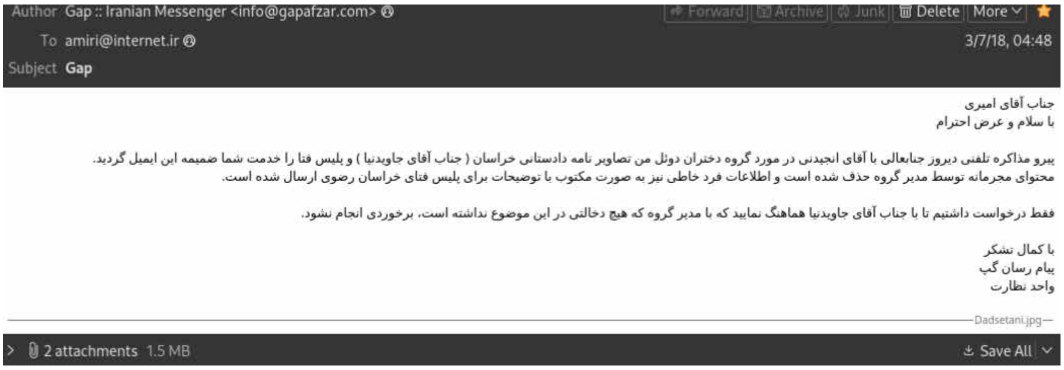


Author s.markolaee@iranmobin.com
To amiri@internet.ir
4/7/18, 05:53
Subject برآورد نیزمندی های او لیه پیام رسان آی گپّ

با سلام
احتراما پیرو مذاکره تلفنی، به پیوست فهرست نیازمندی های برآوردی و اولیه آی گپ در دو حالت یوزر رجیستر و کانکارنت تقدیم می گردد.
با تشکر

1 attachment: Infra Requirements for 1-5-10 M concurrent IGAP Users.pdf 333 KB — Save

Infra Requirements for 1-5-10 M concurrent IGAP Users.pdf 333 KB



Author Gap :: Iranian Messenger <info@gapafzar.com>
To amiri@internet.ir
3/7/18, 04:48
Subject Gap

جناب آقای امیری
با سلام و عرض احترام

پیرو مذاکره تلفنی دیروز جنابعالی با آقای انجیدنی در مورد گروه دختران دوئل من تصاویر نامه دادستانی خراسان (جناب آقای جاویدنیا) و پلیس فتا را خدمت شما ضمیمه این ایمیل گردید.
محتوای مجرمانه توسط مدیر گروه حذف شده است و اطلاعات فرد خاطی نیز به صورت مکتوب با توضیحات برای پلیس فتای خراسان رضوی ارسال شده است.

فقط درخواست داشتیم تا با جناب آقای جاویدنیا هماهنگ نمایید که با مدیر گروه که هیچ دخالتی در این موضوع نداشته است، برخوردی انجام نشود.

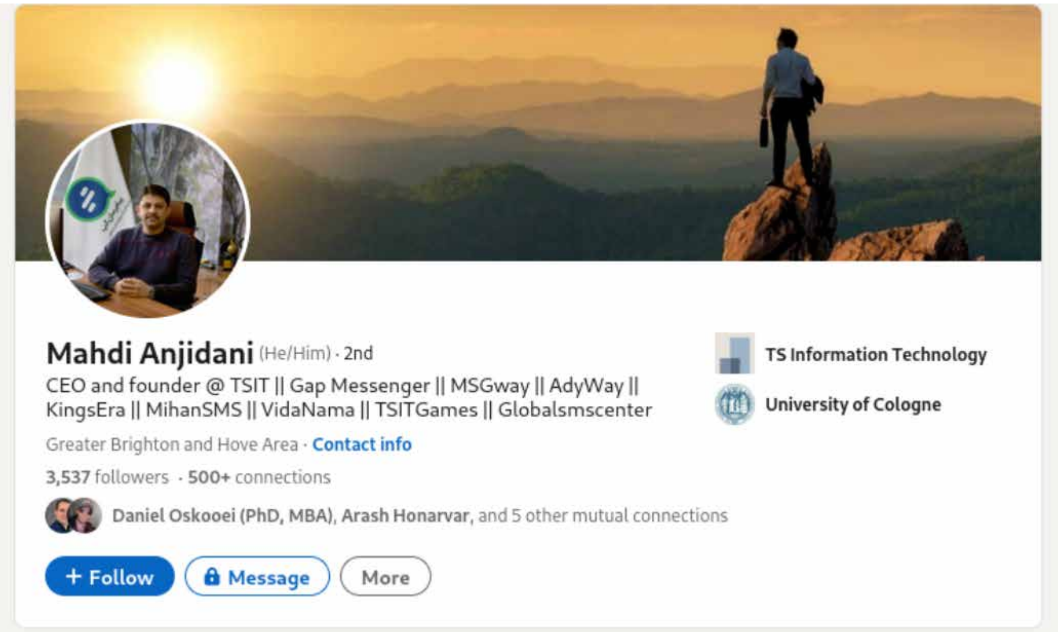
با کمال تشکر
پیام رسان گپ
واحد نظارت

Dadsetani.jpg

2 attachments 1.5 MB
Save All

Based on the information publicly available on Mehdi Engidni's LinkedIn account, it is mentioned that he is not only the manager of the mentioned messenger but also the founder of another company named TS Information Technology located in England.

Information on the UK government's company registration website confirms that he is a director of the company.

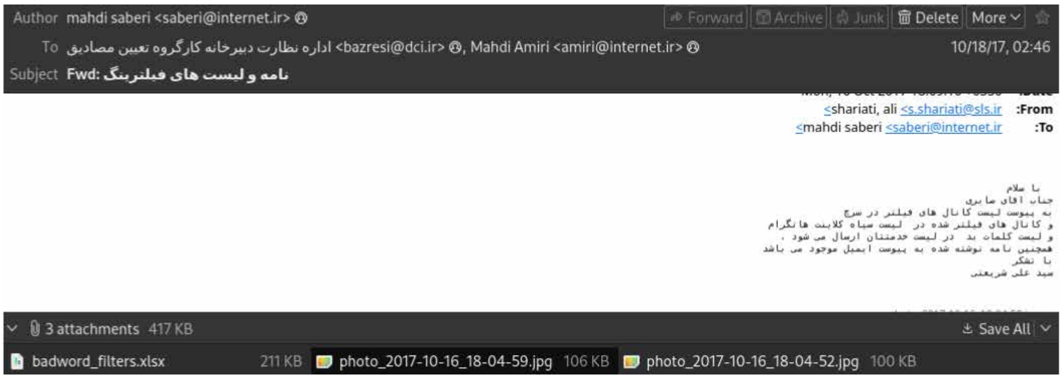


Mahdi Anjidani (He/Him) · 2nd
CEO and founder @ TSIT || Gap Messenger || MSGway || AdyWay || KingsEra || MihanSMS || VidaNama || TSITGames || Globalsmscenter
Greater Brighton and Hove Area · Contact info
3,537 followers · 500+ connections
Daniel Oskooei (PhD, MBA), Arash Honarvar, and 5 other mutual connections
TS Information Technology
University of Cologne

Golden Telegram

Golden Telegram was a fraudulent application that, according to Iranian officials, was made from Telegram under the supervision of security officials. This application was later removed from Google Play due to eavesdropping and privacy violations.Telegram also issued a warning message to users of this application.

In the letters (link 1, 2) that this company sent to the Attorney General's



Author mahdi saberi <saberi@internet.ir>
To اداره نظارت دبیرخانه کارگروه تعیین مصادیق <bazresi@dci.ir>, Mahdi Amiri <amiri@internet.ir>
10/18/17, 02:46
Subject Fwd: نامه و لیست های فیلترینگ

Mon, 16 Oct 2017 18:09:16 +0330 :Date
<shariati, ali <s.shariati@sls.ir :From
<mahdi saberi <saberi@internet.ir :To

با سلام
جناب اقای صابری
به پیوست لیست کانال های فیلتر در سرج
و کانال های فیلتر شده در لیست سیاه کلاینت ها تگرام
و لیست کلمات بد در لیست خدمتتان ارسال می شود .
همچنین نامه نوشته شده به پیوست ایمیل موجود می باشد
با تشکر
سید علی شریعتی

3 attachments 417 KB
badword_filters.xlsx 211 KB
photo_2017-10-16_18-04-59.jpg 106 KB
photo_2017-10-16_18-04-52.jpg 100 KB

Office, they have highlighted the capabilities of Golden Telegram, including word and channel Internet blocking and censoring, blacklisting clients, as well as detecting obscene text and immoral images.

Before this, on November 21, 2017, the Center for Human Rights published a report outlining the technical capabilities of Golden Telegram to censor content based on keywords and channels.

Conclusion

This report has investigated the Internet control and surveillance in Iran, based on the analysis of over 80,000 leaked emails pertaining to the WGDICC from 2014 to 2022. The report has revealed how various actors and entities are involved in the development and implementation of Iran's digital policy, which aims to restrict access to information, monitor online activities, and suppress dissent. The report has also examined how these forces are advancing a drive by the Iranian government to develop a "national internet" and consolidate its control over the online activities of its citizens.

The report has confirmed what we have long warned: that sanctions have contributed to the creation of a national intranet in Iran, by forcing users to rely on local services and apps, such as Gap and Rubika, that are subject to censorship and surveillance. The report has also shown that this is a trend that has been going on for years, as the Iranian government has been empowering local infrastructure and app developers to infringe upon the rights of Iranians. Therefore, we urge the US, UK, EU, and UN to reconsider their sanctions policies and open up the space for Iranians to access a free and secure internet. We also urge tech companies, civil society organizations, and Internet freedom groups to collaborate and support Iranians in their quest for digital rights.