

09 January 2021

Deep Dive into the “Indian Chronicles” Saga and Way Forward for Pakistan

Author: Zaki Khalid*

Key Points:

- Hard-hitting official statements and a frenzied media blitzkrieg aside, the emergence of the web-based technologies provide an added layer of discreetness and deniability when conducting aggressive targeted attacks against Pakistan's integrity.
- While EU (European Union) DisinfoLab's report names several individuals in whose name various website domains were registered, many of them were unidentifiable and untraceable, leading to strong speculations that they are fake identities or “avatars”.
- Apart from the media and publishing services, the Srivastava Group's less-known company, Aglaya, marketed itself as a vendor of hacking/espionage tools. This wholly different vertical of tradecraft adds a more sophisticated yet discreet dimension to the Srivastava family's activities.
- Additional open-source findings indicate that the company was involved in projects for the Indian Armed Forces.
- The surprisingly uninterrupted continuity of the Srivastava Group's influence operations clearly points toward independence from a particular political regime's patronage.
- The most plausible working hypothesis amidst this paradox is that the Srivastava Group is a non-state group/actor that builds and operates a network of physical and digital assets (“fronts”) to provide “services” for clients including various political regimes in the Union Government (New Delhi). The fact that it is not “state-owned”, per se, explains its continued existence.
- The financing of the dubious Non-Governmental Organisations (NGOs), its “research” staff, campaign logistics and material requires access to the discreet supply chain networks traditionally nurtured by intelligence agencies. In terms of the defined mandates, only the Research and Analysis Wing (R&AW) is sanctioned to conduct overseas operations.
- A dedicated cell of skilled fact-checkers and open-source intelligence specialists should be inducted within the External Publicity Wing in the Ministry of Information & Broadcasting through the lateral entry to proactively monitor, identify and counter the organised groups, publishing disinformation and propaganda against Pakistan's diplomatic, cultural and economic interests.

*Zaki Khalid is a strategic analyst and freelance commentator based in Rawalpindi, Pakistan. His areas of interest include national security, geopolitics, cyberspace and maritime affairs. He is also the founder and editor of “Pakistan Geostrategic Review (PGR)”, an independent platform publishing a premium newsletter and podcasts on geostrategic developments.

The Indian security establishment's involvement in the activities that are detrimental to Pakistan's national security and foreign policy interests is indubitable. It has remained persistent since the partition of undivided India in 1947. Other state and non-state actors are also involved in destabilising activities, but contrary to claims, India retains its perilous obsession¹ with Pakistan.

Hard-hitting official statements and a frenzied media blitzkrieg² aside, the emergence of the web-based technologies provides an added layer of discreetness and deniability when conducting aggressive targeted attacks against the State of Pakistan's integrity. In this context, the recent EU DisinfoLab's report³ mapping 15 years of disinformation operations by the Srivastava Group provides important takeaways that need to be examined thoroughly.

This paper explores the selected aspects of the Srivastava Group's history and operations, building further on the existing information already compiled by the EU DisinfoLab. As such, the readers are advised to read it to understand the context of the comments mentioned herein. The paper concludes with recommendations for the Government of Pakistan that can take this issue to its logical conclusion and pre-empt such organised campaigns in the future.

Overseas Front Persons

While the EU DisinfoLab's report names several individuals in whose name various website domains were registered, many of them were unidentifiable and untraceable, leading to strong speculations that they are fake identities or "avatars". Through rigorous open-source research, three known domain name registrants based in Europe and Canada were identified (see **Figure 1**).

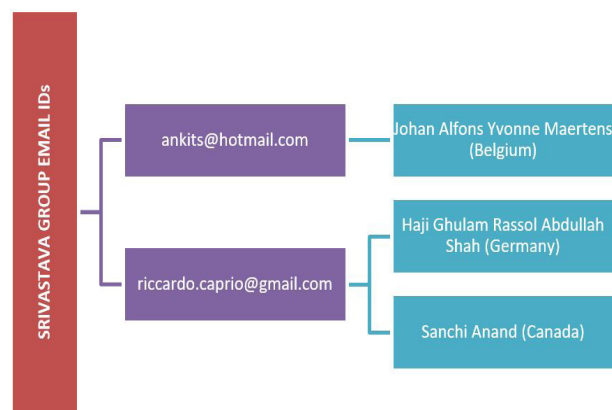


Figure 1 – Author's plotting of links between email IDs and identified/real front persons for the Srivastava Group

1. Johan Alfons Yvonne Maertens (Belgium)

The official website of the South Asia Democratic Forum (SADF) is registered against the email ID *csopus@yahoo.com*, also used to register domain names for the fake NGOs namely International Forum for Rights and Security (IFFRAS) and the European Organisation for Pakistani Minorities (EOPM). The same email ID was also used to register a domain name *jucheidea.com* for the International Council For Juche Idea in New York (United States).⁴ The registrant name Johan Maertens is the same as that of the person who is the Co-Director⁵ of the International Imam Organisation, with Ankit Srivastava.⁶ Maertens' full/ legal name is Johan Alfons Yvonne Maertens, a Belgian psychotherapist⁷ who is the Director of De Sleutel Network in Belgium. Concurrently, he is the Chair of the Scientific Committee of the Rotary Action Group for Addiction Prevention (RAG AP)⁸ which also has a presence in Pakistan. Maertens has also remained the Managing Director of a shady company named Energy for Sustainable Action (Enforsa)⁹ which operates in Belgium, Italy, Rwanda and India.¹⁰ Evidence shows that he is not just a domain name registrant for the Srivastava Group but also a functional/active member of the so-called International Council for Inter-Religious Cooperation (ICIRC) as the Vice President¹¹, participating in

⁴ "csopus@yahoo.com", *Domain Big Data*, <https://archive.vn/UZOC6>.

⁵ "International Imam Organisation", *Kruispuntbank van Ondernemingen*, <https://archive.vn/Oq7uA>.

⁶ "csopus@yahoo.com", *All People*, <https://archive.vn/6sSKJ>.

⁷ "Johan Maertens", *LinkedIn*, <https://www.linkedin.com/in/johan-maertens-11975411/>.

⁸ "Scientific Committee", *Rotary Action Group for Addiction Prevention*, <https://archive.vn/l60U8>.

⁹ "The Team", *Enforsa*, <https://archive.vn/1GZzf>.

¹⁰ "Enforsa India Private Limited", *Indian Company*, last modified January 27, 2020, <https://archive.vn/3MjAD>.

¹¹ "Michael Theurer Hosts Inter-Religious Dialogue: Increasing the Understanding Between Islam and the West", *CISION PR Newswire*, June 12, 2010, <https://www.prnewswire.com/news-releases/michael-theurer-hosts-inter-religious-dialogue-increasing-the-understanding-between-islam-and-the-west-96207264.html>.

¹ Nissim Mannathukkaren, "India's perilous obsession with Pakistan", *The Hindu*, last modified April 24, 2019, <https://www.thehindu.com/opinion/op-ed/indias-perilous-obsession-with-pakistan/article26925287.ece>.

² Kumar Ketkar, "Indian media's obsession with Pakistan and Imran Khan is to serve a bigger purpose", *The Print*, last modified October 7, 2019, <https://theprint.in/opinion/indian-media-obsession-pakistan-imran-khan-narendra-modi/302031/>.

³ "Indian Chronicles: Deep Dive into a 15-Year Operation Targeting the EU and UN to Serve Indian Interests", *EU Disinfo Lab*, last modified 9 December 2020, <https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/>.

conferences at the European Parliament.

2. Haji Ghulam Rassol Abdullah Shah (Germany)

This Afghan businessman in Germany has 16 website domains registered on his name, i.e. Abdullah Shah, including specific domain names targeting the Maldivian government, such as *maldivesaffairs.com* and *maldivesaffair.com*.¹² Interestingly, these two domain names also identify Riccardo Caprio as the registrant¹³, and both use the same email ID (*riccardo.caprio@gmail.com*).¹⁴ The email ID *riccardo.caprio@gmail.com* was also used to register the website of European Organization for Pakistani Minorities (EOPM), set up in 2010.¹⁵ A closer inspection of the other website domains registered in Shah's name reveals his direct association with *rehmatsgmbh.com*, associated with REHMATS Im-Export GmbH, a wholesale dealer of commercial vehicles based in Hamburg, Germany.¹⁶ Abdullah Shah himself is the Managing Director of this concern while another Afghan-origin individual, Rehmat Ullah, is a partner. Another domain *ghaznimotors.com* is associated with Ghazni Motors Free Zone Company (FZCO) based in Dubai, United Arab Emirates (UAE)¹⁷; this concern also deals with the sale of vehicles and is by one Ali Reza Abdul Hakim.¹⁸ There are reasons to suspect that REHMATS (Germany) may be linked to Ghazni Motors (UAE).

3. Sanchi Anand (Canada)

The email ID used in the name of Abdullah Shah (*riccardo.caprio@gmail.com*) was also used to register a fake news website South Asia News on a Canada-hosted domain name in 2012 (*sanews.ca*). The registrant name mentioned in this domain is Sanchi Anand. Open-source research revealed that a month before registering this domain name, Ankit's spouse Neha Srivastava set up a company named Great Cause Foundation in Canada, in which she remains a Director alongside Priya Mehandru and one Sanchi Anand¹⁹. Further research indicates Sanchi is a former Indian-origin Accounting Technician at MacEwan University

¹² "List of domain names registered by Abdullah Shah", *Domain Big Data*, <https://archive.vn/3jZVs>.

¹³ "Riccardo.Caprio@gmail.com", *Domain Big Data*, <https://archive.vn/CjvXX>.

¹⁴ "maldivesaffairs.com", *Domain Big Data*, <https://archive.vn/orfRN>.

¹⁵ "eopm.org stats and valuation", *WebsiteOutlook*, last modified May 3, 2018, <https://archive.vn/Ulud6>.

¹⁶ "REHMATS Im-Export GmbH", *D&B Business Directory*, <https://archive.vn/oU95F>.

¹⁷ "Contact Us", *Ghazni Motors FZCO*, <https://archive.vn/lvW5V>.

¹⁸ Google search terms "Ali Reza Abdul Hakim" (quotation marks included).

¹⁹ "Great Cause Foundation", *OpenCorporates*, last modified October 2, 2020, <https://opencorporates.com/companies/ca/8130795>.

based in Edmonton, Canada²⁰.

On the basis of the information shared above, it is reasonably believed that the companies with which Johan Alfons Yvonne Maertens (Belgium), Haji Ghulam Rassol Abdullah Shah (Germany/United Arab Emirates) and Sanchi Anand (Canada) are affiliated may be used as conduits for financial transactions by the Srivastava Group to fund overseas operations.

North Korean Links

Why the Srivastava Group would register a company and domain name for the "Juche Idea" (political philosophy of North Korea) seems odd. A detailed report by Devirupa Mitra for *The Wire* examines the direct historical relations between the Srivastava family and the North Korean regime. Reportedly, the Srivastava Group's founder Dr Govind Narain Srivastava (Ankit's father) was a longtime Secretary-General of the Asian Regional Institute of the Juche Idea, which promoted the ideals of the Juche thought in the Indian subcontinent.²¹

Dr Srivastava was a documented journalist²² who participated in several Juche conferences, including the 1997 International Seminar of 21st Century and Position of Human Being in Tokyo to pay homage to late North Korean leader Kim Il-Sung.²³ Some of his authored books include *Non-Alignment and New International Economic Order* (1988)²⁴, *Peace, Security, and Non-alignment: Asian Dimension* (1988)²⁵, *NAM and the New International Information and Communication Order* (1989)²⁶ and *Policy of Non-Alignment: Bandung to Cartagena* (1995).²⁷ These publications indicate that the Srivastava family's patron had not just covered various Non-Aligned Movement (NAM) events but played a crucial role in its popularity and outreach.

²⁰ "Sanchi Anand", *LinkedIn*, <https://www.linkedin.com/in/sanchi-anand-5555b869>.

²¹ Devirupa Mitra, "Man Behind Institute Which Sponsored MEPs' Kashmir Visit Had Close Ties With North Korea", *The Wire*, last modified November 1, 2019, <https://thewire.in/world/srivastava-group-north-korea>.

²² "Leadership", *International Institute for Non-Aligned Studies*, <https://iins.org/leadership/>.

²³ Cameron W. Barr, "Late Dictator Teaches Self-Reliance", *The Christian Science Monitor*, last modified February 10, 1997, <https://www.csmonitor.com/1997/0210/021097.intl.intl.5.html>.

²⁴ "Non-Alignment and New International Economic Order", *Amazon*, <https://www.amazon.com/Non-Alignment-New-International-Economic-Order/dp/8171280161>.

²⁵ "Peace, Security, and Non-alignment: Asian Dimension", *Google Books*, https://books.google.com.ua/books/about/Peace_Security_and_Non_alignment.html?id=OHOLAAAIAAJ.

²⁶ "NAM and the New International Information and Communication Order", *Amazon*, <https://www.amazon.com/NAM-International-Information-Communication-Order/dp/8171280269>.

²⁷ "Policy of non-alignment : Bandung to Cartagena", *Catalogue of the National Library of Australia*, <https://catalogue.nla.gov.au/Record/1613539>.

These historical links to North Korea, however, appear distinct from the Srivastava Group's activities in Europe and elsewhere.

Maertens' business engagements in Enforsa add another layer of discreet stakes with India. These have not been explored in detail and could, to a great extent, provide insight into the financial and logistical network used to fund demonstrations and influence operations against Pakistan. As Mitra reveals in her report for *The Wire*, the Srivastava Group did not have a "healthy" balance sheet.

Aglaya and Services for India's Security Establishment

Apart from the media and the publishing services, the Srivastava Group's less-known company Aglaya marketed itself as a vendor of hacking/espionage tools. This wholly different vertical of tradecraft adds a more sophisticated yet discreet dimension to the Srivastava family's activities.

This author's open-source intelligence scan reveals that the company's registered name is Aglaya Scientific Aerospace Technology Systems Private Limited, active since November 2014 in New Delhi.²⁸ The company has five Directors, including Dr Ankur Srivastava (Ankit's brother) and his spouse Ratna Srivastava. Dr Ankur's link to the Srivastava Group can also be established through his official company email ID (ankur@aglaya.com) registered in the same physical address as the Srivastava Group,²⁹ and particularly his brother Ankit's various businesses.

At the 2015 edition of ISS World Middle East in the UAE, a leading platform for intelligence and surveillance technologies, Dr Ankur conducted two technical workshops including a live presentation on "asymmetric warfare" using remote cyber weapons delivery.³⁰ In a subsequent interview, he "regretted" attending the seminar as he was "never able to close a deal and sell its (Aglaya's) services".³¹ While this may have been true, other reports reveal that the defunct UAE-based cyber company DarkMatter, notorious

for conducting state-sponsored hacking operations³², outsourced some of its offensive targetings to Aglaya, a fact acknowledged by Dr Ankur himself.³³

Dr Ankur's current designation is the Director of the Institute for Systems Research³⁴ and its associated IDEALab³⁵ at the University of Maryland, (US) that is sponsored by the likes of Defence Advanced Research Projects Agency (DARPA), Air Force Office of Scientific Research and Office of Naval Research, to name a few.³⁶ At the 2016 edition of Defence Expo (DefExpo) India, Aglaya marketed itself as Aglaya (Cyber Warfare Labs)³⁷ and performed a live demo of its Over-The-Air Wireless Electricity Transmission (WET) technology.³⁸ There was apparently no response to the appeals for funding in 2016³⁹ which is probably why Dr Ankur appears to have re-appealed for funds through a new company named Defence Security and Tactical Systems (DSATS) in 2018⁴⁰

Cybersecurity commentator, Eliza Miranda, observed that whether it is Aglaya or DSATS, "both were a part of the desperate measures taken by Ankur Srivastava in desperate times. The PhD holder from UCLA only needed a source of surplus outside funding for his project focused on the 'Wireless Electricity Transmission for Defence and Intelligence Deployment'. Nevertheless, the path that Srivastava chose to acquire those funds for his project fell back on him".⁴¹ While it may seem that Aglaya's fate was sealed and there may not have been any foreign clients except DarkMatter (UAE), additional open-source findings indicate that the company was involved in projects for the Indian

²⁸ Mark Mazzetti, Adam Goldman, Ronen Bergman and Nicole Perlroth, "A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments", *The New York Times*, last modified March 21, 2019, <https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html>.

²⁹ Sarmin Rahman, "How DarkMatter Used Aglaya and CyberPoint to Build A Shady Surveillance Operation for UAE", *Indie Hackers*, <https://archive.vn/RwYqS/>.

³⁰ "Faculty Directory", *Department of Electrical & Computer Engineering at the University of Maryland*, <https://archive.vn/DitBw>.

³¹ "People", *IDEALab at the University of Maryland*, <https://archive.vn/vG7sj>.

³² "Sponsors", *IDEALab at the University of Maryland*, <https://archive.vn/yO6uo>.

³³ "Eye on Defence April 2016", *Slideshare*, April 9, 2016, <https://www.slideshare.net/agcool/eye-on-defence-april-2016>.

³⁴ Tweet by Aglaya, March 14, 2016, <https://archive.vn/3m0SR>.

³⁵ "Made in India - Aglaya to Release Wireless Electricity Transmission for Defence and Intelligence Deployment at the Indian DefExpo 2016", *CISION PR Newswire*, March 9, 2016, <https://www.prnewswire.com/in/news-releases/made-in-india---aglaya-to-release-wireless-electricity-transmission-for-defence-and-intelligence-deployment-at-the-indian-defexpo-2016-571474461.html>.

³⁶ "Ground breaking innovation of 'Over-the-air' delivery of electricity by DSATS", *PR-Inside*, January 23, 2018, <https://www.pr-inside.com/ground-breaking-innovation-of-over-the-air-deliver-r4674082.htm>.

³⁷ "Spyware to Cyber Nukes: Is Aglaya A Project Proposal of Ankur Srivastava?", *CyberHackNews*, February 7, 2018, <https://archive.vn/RFXyj>.

²⁸ "Aglaya Scientific Aerospace Technology Systems Private Limited", *Zauba Corp*, <https://archive.vn/1cJZ2>

²⁹ "Ankur@aglaya.com", *Domain Big Data*, <https://archive.vn/YvXPW>.

³⁰ "Track 4", *ISS World Training*, https://www.issworldtraining.com/iss_meat/Track4.html.

³¹ Lorenzo Franceschi-Bicchierai, "This Leaked Catalog Offers 'Weaponized Information' That Can Flood the Web", *VICE*, last modified September 2, 2016, <https://www.vice.com/en/article/d7yvvx/leaked-catalog-weaponized-information-twitter-aglaya>.

Armed Forces.

For example, the CV of one Ashish Mathur, a former Cybersecurity Specialist at Aglaya from 2017 to 2018, mentions activities such as the vulnerability assessment and penetration testing for web/mobile applications used by the Indian defence forces. There is also a separate mention of a project undertaken by Aglaya titled “Implementation of Sniffer in GSM Network (Government of India)”. Mathur mentions the project was sponsored by “Special Signals, Tri-Shakti Regiment - Ministry of Defense (sic) - India” which is a reference to the Directorate of Signals Intelligence under India’s tri-service Defence Intelligence Agency (DIA). In the “Honours and Awards” section of his CV, Mathur mentions he was “acknowledged” by the National Technical Research Organisation (NTRO) in 2011, indicating the past employment with India’s premier technical intelligence agency.⁴² It also shows further that Aglaya was undoubtedly working for the Ministry of Defence till 2018.

EU Disinfo Lab’s report mentions how Aglaya marketed itself as a provider of “Information Warfare (IW) services”. Here, it cannot be ruled out that some of the website domains registered by the Srivastava Group were being used as command-and-control servers fetching data from mobile and computer devices of unsuspecting victims targeted by India’s security establishment.

Lobbying at the European Union

In October 2019, two months after New Delhi’s unilateral abrogation of the Articles 370 and 35-A, an unofficial visit of the European parliamentarians to the Indian-Occupied Jammu & Kashmir (IOJ&K) was arranged by Madi Sharma of Women’s Economic and Social Think Tank (WESTT), another front for the Srivastava Group that is financed by the Srivastava family-run International Institute of Non-Aligned Studies (IINS)⁴³.

After this controversial visit, the EU’s then Minister for Foreign Affairs Josep Borrell acknowledged its private status and added that the European External Action Service (EEAS) was “not informed” of the relevant preparations.⁴⁴ United Kingdom’s (UK) then

Minister of European Parliament (MEP) Julie Ward had earlier revealed that 22 out of the 27 MEPs who were nominated to visit India through IINS (4 later backed out) belonged to the right-wing political parties. It included some MEPs that “openly backed the Indian Government’s abrogation of Jammu & Kashmir’s special status”⁴⁵. A month after this private and unofficial visit, Vellamvelly Muraleedharan, the Minister of State in India’s Ministry of External Affairs (MEA), placed on record that the visit was undertaken “at the invitation of IINS” and that MEA had merely “facilitated” it.⁴⁶

This visit to IOJ&K was preceded by a similar stunt in 2018 wherein Madi Sharma organised a private visit for the MEPs to the Maldives to scandalise and discredit the regime of then Maldivian President Abdulla Yameen.⁴⁷ Another visit was arranged the same year to Bangladesh in which the Sharma-led delegation “praised” Sheikh Hasina’s regime for “furthering democracy in Bangladesh”⁴⁸. Not surprisingly, the objective of both these visits reflected the aspirations of India’s strategic establishment, i.e. ensure support against a pro-China Yameen and in favour of Hasina.

Evidently, apart from its elaborate network of digital assets for influence operations, the Srivastava Group also maintains connections with select MEPs who can be lobbied indirectly for the furtherance of New Delhi’s political and diplomatic agendas while generally deceiving people into believing these “initiatives” are of European origin.

Uninterrupted Operations

The surprisingly uninterrupted continuity of the Srivastava Group’s influence operations clearly points toward independence from a particular political regime’s patronage.

At the time of its reported emergence in 2005, the year in which the EU DisinfoLab claims the “Indian Chronicles” began, the Manmohan Singh-led Indian National Congress (INC) government was in its first term in office. Today, the Bharatiya Janata Party (BJP) is almost halfway through its second. More importantly, change of various National Security Advisers and cabinet ministers, who each bring their own personality-based

⁴⁵ “Lack of political balance in an MEP delegation to Kashmir / Controversial visit to Kashmir”, official website of the European Parliament, March 23, 2020, https://www.europarl.europa.eu/doceo/document/E-9-2020-000290_EN.pdf.

⁴⁶ “Question No 1165 European Union Team Visit to Kashmir”, official website of the Government of India’s Ministry of External Affairs, <https://mea.gov.in/rajya-sabha.htm?dtl/32116/QUESTION+NO1165+EUROPEAN+UNION+TEAM+VISIT+TO+KASHMIR>.

⁴⁷ “Influencing Policymakers with Fake Media Outlets - An investigation into a pro-Indian influence network”, *EU Disinfo Lab*, December 2019, <https://perma.cc/AU34-PYT6> (pages 12-14).

⁴⁸ Tweets by Saket Gokhale, October 31, 2019, <https://archive.vn/l3mjE>.

⁴² “Ankur Mathur CV”, archived PDF from LinkedIn profile, https://www.mediafire.com/file/gdyglo59u1syf0b/Ankur_Mathur_CV.pdf/file.

⁴³ Ipsita Chakravarty & Rohan Venkataramakrishnan, “How did an ‘international business broker’ gain access to PM Modi for EU delegates’ Kashmir trip?”, *Scroll*, October 29, 2019, <https://scroll.in/article/942028/how-did-an-international-business-broker-gain-access-to-pm-modi-for-eu-delegates-kashmir-trip>.

⁴⁴ “Answer given by High Representative Borrell”, official website of the European Parliament, March 23, 2020, https://www.europarl.europa.eu/doceo/document/E-9-2020-000290-ASW_EN.pdf.

policies in office, did not exert any known change in the Srivastava Group's operational tactics. But if we examine 1980 (year of IINS' registration) as the starting point of the campaigns, we are talking of almost four decades of survival.

In hindsight, the Singh era was not as aggressive toward Pakistan as the incumbent Narendra Modi's terms in office. But a sampling of prominent fake NGOs and their associated domain names registered by the Srivastava Group (highlighted in EU Disinfo Lab's report) indicates that the registrations (not necessarily activities) were almost double during the INC rule than BJP's (see Annexure-I).

The most plausible working hypothesis amidst this paradox is that the Srivastava Group is a non-state group that builds and operates a network of physical and digital assets ("fronts") to provide "services" for the clients including various political regimes in the Union Government (New Delhi). The fact that it is not "state-owned", per se, explains its continued existence.

It is also evident that the amateur modus operandi adopted by the Srivastava Group to conduct influence operations stands in contrast to the more sophisticated cyber-based and cyber-enabled operations conducted by the Indian state actors.⁴⁹

Income & Business Interests

Per the EU DisinfoLab, the Srivastava family owns approximately 500 website domains. The average annual cost for a domain is \$10.⁵⁰ In this context, the Srivastava Group would need at least \$5000 per annum to retain ownership of these domains alone. This does not include the salaries for the staff members, front persons and other advertising expenses.

Open-source research provides an insight into some known sources of the Srivastava family's income. Dr Pramila Srivastava, her sons Ankit and Dr Ankur and their daughter-in-laws Neha Srivastava and Ratna Srivastava hold Directorships in 17 known companies (12 in India and 5 in Canada).⁵¹ These companies are involved in a variety of sectors, mostly related to education, water/waste management and information service activities, as per the official declarations. One of these, New Delhi Aviations Private Limited, could be mistaken as being part of the aviation and aerospace-related activities when, in fact, it deals in information

services only (see Annexure-II).

The other known source of income is the revenue through website traffic and advertisement exposures via Google AdSense; a brief sampling of the operational websites revealed their analytics and publisher IDs along with the estimated monthly income. Five noteworthy website domains alone have the potential to generate \$50,000+ per month in online ad-based revenue generation (see Annexure-III). While a detailed analysis of network-wide domains is beyond the scope of this paper, it is clear that the maintenance of dynamic websites publishing syndicated content is, in and of itself, also a steady stream of income for the Srivastava Group.

Content published by the Srivastava Group forums, such as SADF etc., contain strategic-level narratives that converge with the interests of India's security establishment and would not generally hold the same commercial appeal as syndicated content does. Here, it would be reasonable to hypothesise that such content is solicited by, or simply published at the behest of, a government organ in New Delhi. As mentioned earlier, companies associated with front persons based in Belgium, Germany and Canada may be serving as conduits to funnel such transactions to and from New Delhi.

If we examine the Behaviours and Content from ABCD (Actors, Behaviour, Content, Distribution) pyramid in the EU DisinfoLab's summary; we can attempt to assess the financial versus public relations (PR) benefits that the Srivastava family could gain through participation in the 'Indian Chronicles'. Open-source research suggests only the dissemination of fake news provides tangible benefits (see Annexure-IV). Therefore, to engage in political and diplomatic activities that carry no tangible returns on investment, an external source of capital would be necessary.

India's Contemporary IW Paradigm – Capabilities & Limitations

There are two functional prongs that engage in state-sanctioned IW campaigns in India. One comes under the Defence Minister, and the other comes directly under the National Security Adviser (See Figure 1).

⁴⁹ The primary argument is the disregard for operational security when registering website domains against personal email addresses.

⁵⁰ Kevin Wood, "How Much Is A Website Domain Name?", *HostGator*, March 4, 2019, <https://www.hostgator.com/blog/how-much-website-domain-name/>.

⁵¹ Summary of open source research conducted by the author.

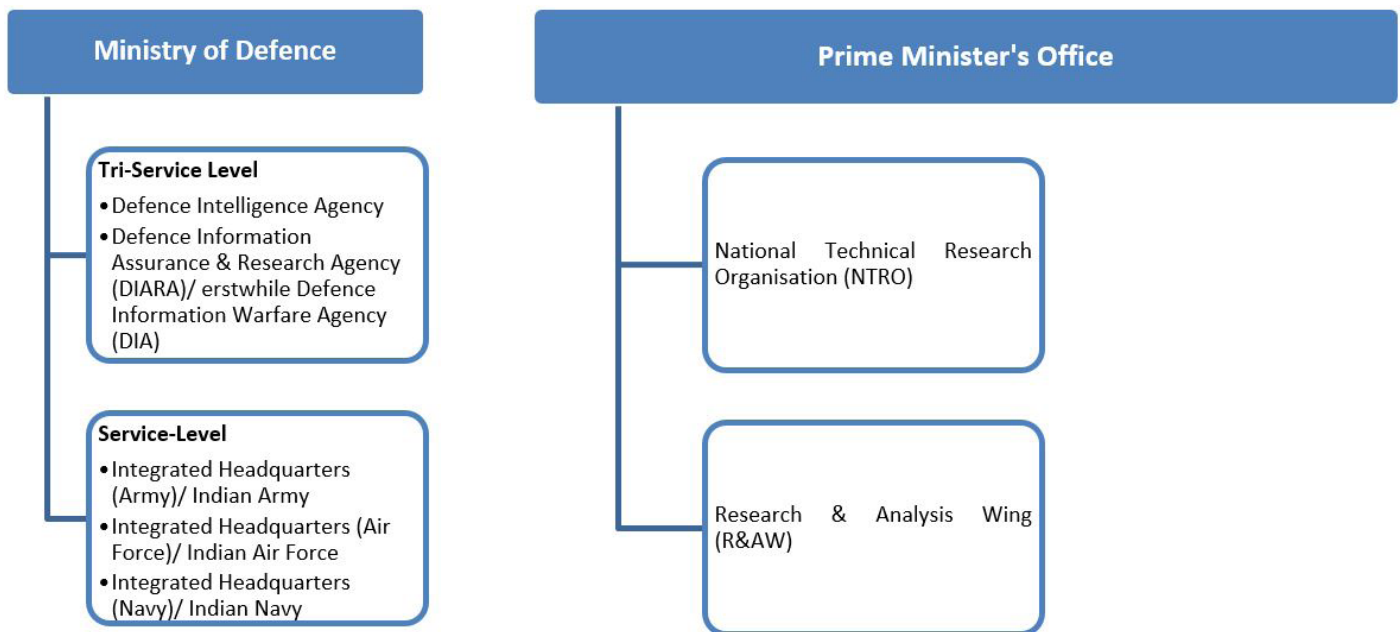


Figure 1 - Author's visual representation of the known Indian state organs engaged in cyber and information operations

Though the Indian Armed Forces do not yet have an updated Joint Doctrine on IW⁵², the conceptual understanding at service levels is more or less the same. IW generally comprises three components, namely Cyber Warfare, Electronic Warfare and Psychological Warfare (See Figure 2).

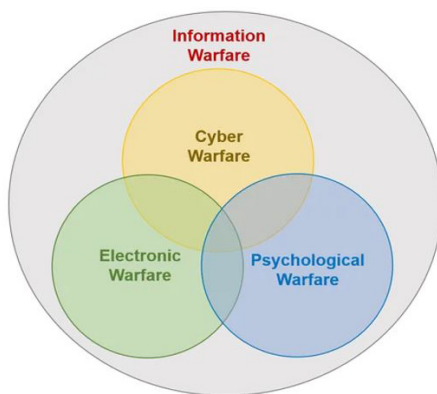


Figure 2 – Elements of India's IW Paradigm⁵³

While the R&AW is known to engage in “ham-handed” psyops⁵⁴ and has acquired “state-of-the-art” gadgets for cyber intelligence⁵⁵, ground operations based primarily on human intelligence remain its forte,

including in Europe.⁵⁶ Lacking the technical expertise and permanent cadre of specialists (unlike NTRO) remains a challenge and could explain the logic of the Srivastava Groups' entry into the equation.

An insightful study by RAND Corporation presents a resourceful breakdown of IW into two distinct areas; Information-Technical Operations (ITO) that comprise modes of delivery to target machines, and Inform & Influence Operations (IIO) comprising the content for messaging to target human minds.⁵⁷ Consolidating the various Srivastava Group websites (IIO) and Aglaya's solutions (ITO) offers an integrated IW package for the end-user.

When we add ground activities through various “fronts” into the mix (physical dimension), such as those carried out by ICIRC, WESTT and SADF, to name a few, the scope of operations extends beyond the declared mandate and the territorial confines of the Indian Armed Forces. The financing of dubious NGOs, its “research” staff, campaign logistics and material requires the access to discreet supply chain networks traditionally nurtured by the intelligence agencies. In terms of defined mandates, only the R&AW is sanctioned to conduct overseas operations.

⁵² Lieutenant General (Retired) RS Panwar, “Towards an Effective and Viable Information Warfare Structure for the Indian Armed Forces”, *The United Service Institution of India*, 2018, <https://usiindia.org/publication/usi-journal/towards-an-effective-and-viable-information-warfare-structure-for-the-indian-armed-forces/>.

⁵³ Lieutenant General (Retired) RS Panwar, “IW Structures for the Indian Armed Forces”, *Future Wars*, March 31, 2020, <http://futurewars.rspanwar.net/iw-structures-for-the-indian-armed-forces-part-i/>.

⁵⁴ Rahul Bedi, “Book Review: Inside RAW, India's ‘Joke and Dagger’ Agency”, *The Wire*, September 22, 2020, <https://thewire.in/books/yatish-yadav-raw-intelligence-agency-book-review>.

⁵⁵ “R&AW steps up vigil, cripples China-Pak nexus in Arabian Sea region (IANS Exclusive)”, *Outlook India*, last modified June 29, 2019, <https://www.outlookindia.com/newscroll/rampaw-steps-up-vigil-cripples-chinapak-nexus-in-arabian-sea-region-ians-exclusive/1564719>.

⁵⁶ Yatish Yadav, “R&AW covert ops dismantled Jamaat-e-Islami terror camps in 1992, reveals spymaster Amar Bhushan in book”, *First Post*, June 30, 2018, <https://www.firstpost.com/india/raw-covert-ops-dismantled-jamaat-e-islami-terror-camps-in-1992-reveals-spymaster-amar-bhushan-in-book-4636441.html>.

⁵⁷ Isaac R. Porche III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, Bruce J. Held, “Redefining Information Warfare Boundaries For An Army In A Wireless World”, *RAND Corporation*, 2013, https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf (see Summary at xxi).

Pakistan's Official Reaction

The Government of Pakistan's reaction to the "Indian Chronicles" saga is circumspect. Prime Minister Imran Khan urged the international community to "take notice" of a "rogue Indian regime" (a reference to the BJP).⁵⁸ Special Assistant to the Prime Minister on National Security Division & Strategic Policy Planning also echoed condemnation of India.⁵⁹ In its press release, the Ministry of Foreign Affairs (MoFA) urged the EU, United Nations Human Rights Council (UNHRC), Belgium and Switzerland to "investigate" into and take "full cognisance" of the EU DisinfoLab's report⁶⁰, messaging that was neither unusual nor extraordinary.

Clearly, the report by the EU DisinfoLab was not dissected in detail, nor is there stated intent to follow through and take the 'Indian Chronicles' saga to its logical conclusion.

Fundamentally, it needs to be understood that the Srivastava Group is a non-state actor that routinely engages with the Government of India; it cannot, however, be construed as a state-sanctioned entity. Instead of isolating one of its users and benefactors, the Government of Pakistan should focus on the Srivastava family's business concerns and take steps to "wrap up" their technical and financial network through collaboration with the international community.

Recommendations

1. Immediate Steps

- Constitution of a Fact-Finding Committee in the Prime Minister's Office comprising members from, but not limited to, the Foreign Affairs, Defence, Interior, Information Technology and Law & Justice ministries. The committee should be empowered to liaise directly with foreign and interior/ homeland security departments in Canada, Belgium, Germany and Switzerland for the acquisition of requisite documents alongside the EU and UNHRC.
- The committee should task a panel of experienced financial crime investigators, open-source intelligence specialists and international law experts to thoroughly

⁵⁸ Naveed Siddiqui, "Revelations about Indian disinformation network vindicate Pakistan's stance: PM Imran", *Dawn*, last modified December 11, 2020, <https://www.dawn.com/news/1595035/revelations-about-indian-disinformation-network-vindicate-pakistans-stance-pm-imran>.

⁵⁹ Tweets by Dr Moeed W. Yusuf, December 9, 2020, <https://archive.vn/mo7rg>.

⁶⁰ "Rejection of Indian attempts to deny responsibility of disinformation campaign against Pakistan", *official website of the Government of Pakistan's Ministry of Foreign Affairs*, <http://mofa.gov.pk/rejection-of-indian-attempts-to-deny-responsibility-of-disinformation-campaign-against-pakistan/>.

analyse multi-source information and compile its final report.

- A list of individuals and entities involved in the campaigns should form the bedrock of this report. Srivastava family's key business stakeholders and accomplices based overseas should be prosecuted as "malicious cyber actors" through liaison with INTERPOL.
- Secretary (Information Technology) at the Ministry of Information Technology & Telecommunication (MoITT) should initiate a high-level discussion with the Internet Corporation for Assigned Names and Numbers (ICANN) to raise the issue of insufficient regulatory oversight by the domain registrars that helped the Srivastava family evade regulatory compliance (*domainpeople.com*, *godaddy.com* etc.).
- Highlights of the committee report should be raised by Pakistan's Permanent Representative to the United Nations (UN).
- Pakistan's Representative in the Shanghai Cooperation Organisation (SCO) should share the final dossier prepared by the committee with the Secretary-General of SCO's Regional Anti-Terrorist Structure (RATS) to ensure that the Srivastava family's businesses/assets and individuals involved are included in the RATS' databank in the light of Article 6, Section 4 of the Agreement on RATS between the member states.⁶¹ This should be followed with a special session on tackling disinformation by the state and non-state actors based in the member states. MoFA will have to take the initiative through coordination with the SCO RATS Council Secretariat.

- The Foreign Secretary should write a letter to the South Asian Association for Regional Cooperation (SAARC) Secretariat urging the establishment of a Regional Task Force to Combat Disinformation similar to the EU's East StratCom Task Force (ESCTF). Pakistan's push for this initiative will bind the regional governments to develop a check-and-balance mechanism against the non-state actors used for targeting the political, diplomatic and economic interests of the member states.

- The Digital Media Wing (DMW) that was set up within the Ministry of Information & Broadcasting was mandated for positive image-building of Pakistan and for combatting "fake/libellous news".⁶² Its functions need to work on a 24/7 basis to proactively monitor

⁶¹ "Agreement on Regional Anti-Terrorist Structure between the Member States of the Shanghai Cooperation Organisation", <http://eng.sectsc.org/load/207250/>.

⁶² Abdul Qadir, "Digital media wing established to promote national narrative of Pakistan", *ARY News*, last modified October 28, 2020, <https://arynews.tv/en/digital-media-wing-national-narrative-pakistan-propaganda/>.

hostile influence actors and regularly share their findings with concerned law enforcement authorities for further investigation.

- Individuals/entities of Pakistani-origin that benefited financially and politically from the Srivastava Group's assets should be prosecuted under relevant laws of the State of Pakistan.

2. Long-Term Measures

- The Government of Pakistan in association with the parliamentarians should strive for legislation that can provide measures against the foreign-origin disinformation.
- A dedicated cell of skilled fact-checkers and open source intelligence specialists should be inducted within the External Publicity Wing in the Ministry of Information & Broadcasting through the lateral entry to proactively monitor, identify and counter organised groups publishing disinformation and propaganda against the State of Pakistan's diplomatic, cultural and economic interests. Content monitoring related to "national security" or "law and order" should remain under the watch of the Defence and Interior Ministries, respectively, to avoid overlaps.
- A new post of a Director (External Liaison) should be created within the MoITT for streamlined engagements with the regulatory officials and technology companies based overseas.

Prominent Fronts Setup by the Srivastava Group during various Union Governments

Data compiled from the EU DisinfoLab's report and an independent domain WHOIS' investigations by the author.

Year	Front	Website	Union Government
<u>1998</u>	United Indian Websites (UIW)	uiw.net	BJP
<u>2003</u>	DEF CONSULT	defconsult.com	BJP
<u>2005</u>	World Environment and Resources Council (WERC)	-	INC
<u>2005</u>	EP Today	eptoday.com	INC
<u>2005</u>	South Asia Diary	southasiadiary.com	INC
<u>2006</u>	Friends of Pakistan	friendsofpakistan.eu	INC
<u>2006</u>	Kashmir Centre	kashmircentre.eu	INC
<u>2006</u>	Human Rights Council	humanrightscouncil.net	INC
<u>2009</u>	NGO Coordinating Committee on Human Rights (NCCHR) (Maria Rutowicz)	ncchr.org	INC
<u>2010</u>	Pakistani Women's Human Rights Organisations (PWHRO)	pakistaniwomen.org	INC
<u>2010</u>	South Asia Peace Forum	southasiapeaceforum.com	INC

<u>2010</u>	Perspective South Asia	perspectivesouthasia.com	INC
<u>2010</u>	Gilgit News	gilgitnews.net	INC
<u>2010</u>	Gilgit Post	gilgitpost.net	INC
<u>2011</u>	South Asia Democratic Forum (SADF)	sadf.eu	INC
<u>2011</u>	Tehreek-e-Islam	tehreekeislam.net	INC
<u>2012</u>	Commission to Study the Organization of Peace (CSOP)	csopus.com	INC
<u>2012</u>	Friends of Gilgit-Baltistan (FOGB)	fogb.eu	INC
<u>2012</u>	South Asia Revealed	southasiarevealed.com	INC
<u>2012</u>	South Asia News	sanews.ca	INC
<u>2012</u>	Baloch News	balochnews.com	INC
<u>2012</u>	Maldives Affairs	maldivesaffairs.com	INC
<u>2012</u>	Maldives Current	maldivescurrent.com	INC
<u>2013</u>	Baluchistan House	baluchistanhouse.com	INC
<u>2013</u>	EU Chronicle	eu-chronicle.eu	INC
<u>2013</u>	PR News Distribution	prnewsdistribution.com	INC
<u>2013</u>	Euro Consult Inc.	euroconsultinc.com	INC
<u>2013</u>	Pro Lex Publishing	prolexpublishing.com	INC
<u>2014</u>	Balochistan Today	balochistantoday.org	INC
<u>2014</u>	Noida Publishing House	noidapublishinghouse.com	BJP
<u>2016</u>	International Club for Peace Research (ICPR)	icpr-eu.com	BJP
<u>2016</u>	United Schools International (USI)	uso-usi-india.org	BJP
2016	Centre for Environmental and Management Studies (CEMS)	cemstudies.org	BJP
2016	Canners International Permanent Committee (CIPC)	cipcngo.com	BJP

2016	Pan African Union for Science and Technology (PAUST)	paufst.com	BJP
2016	International Association for Democracy in Africa (IADA)	iadafrica.com	BJP
2016	European Union News Network (Arndt Faber)	eunewsagency.com	BJP
2017	Gilgit Times	gilgittimes.com	BJP
2018	AN Consults	anconsults.com	BJP
2019	Four News Agency	fournewsagency.com	BJP

Annexure-II

Known Company Directorships of the Srivastava Family Members

Data compiled by the author through multiple business registry databases in India and Canada.

Year	Name/ Local Registration Number	Country	Type	Directors
1982	Monarch Controls Private Limited (Active) Corporate Identification Number: U74899DL1982PTC014200	India	Other business activities	1. Dr Ankur Srivastava 2. Ratna Srivastava
2008	New Delhi Aviations Private Limited (Active) Corporate Identification Number: U63040DL2008PTC176316	India	Information service activities	1. Ankit Srivastava 2. Dr Pramila Srivastava
2009	River Site Power Private Limited (Struck-off) Corporate Identification Number: U40108DL2009PTC189798	India	Water and waste management activities	1. Sunil Dang 2. Dr Pramila Srivastava
2011	Srivastava Medicare Private Limited (Active) Corporate Identification Number: U85110DL2011PTC226507	India	Primary Education	1. Ankit Srivastava 2. Neha Srivastava
2011	Times Cabs Private Limited (Struck-off) Corporate Identification Number: U63000DL2011PTC224079	India	Information service activities	1. Ankit Srivastava 2. Tarun Wadhwa 3. Devi Prasad (Maya Devi Gupta)
2012	Great Cause Foundation (Active) Corporation Number: 8130795	Canada	Not known	1. Neha Srivastava 2. Priya Mehandru 3. Sanchi Anand

2012	ANR Health Care Private Limited (Active) Corporate Identification Number: U85100DL2012PTC237744	India	Primary education	1. Ankit Srivastava 2. Neha Srivastava
2013	Atlas Aggregates Private Limited (Struck-off) Corporate Identification Number: U14200DL2013PTC247435	India	Manufacturing of wearable apparels	1. Ankit Srivastava 2. Gagan Shukla
2013	Kaya Health Care Private Limited (Struck-off) Corporate Identification Number: U85100DL2013PTC248494	India	Primary education	1. Ankit Srivastava 2. Priyamvada Tripathi 3. Vicky Batra 4. Anil Kumar Lal
2014	A2N International Trading Corporation (Active) Corporation Number: 8887276	Canada	Not known	1. Ankit Srivastava 2. Neha Srivastava
2014	Aglaya Scientific Aerospace Technology Systems Private Limited (Active) Corporate Identification Number: U74110DL2014PTC273228	India	Legal, accounting and book-keeping	1. Dr Ankur Srivastava 2. Ratna Srivastava 3. Inder Mohan Jain 4. Mani Kant Jain 5. Ritu Jain
2015	A2N Broadcasting Private Limited (Active) Corporate Identification Number: U74140DL2015PTC278024	India	Specialised design activities	1. Ankit Srivastava 2. Neha Srivastava
2015	9362967 Canada Ltd (Active) Corporation Number: 9362967	Canada	Not known	1. Ankit Srivastava
2017	Global Weblogics Solutions Inc. (Active) Corporation Number: 10135771	Canada	Not known	1. Ankit Srivastava
2018	Srivastava Group Private Limited (Active) Corporate Identification Number: U74999DL2018PTC337586	India	Professional, scientific and technical activities	1. Ankit Srivastava 2. Neha Srivastava

2019	A2N Energy Private Ltd (Active) Corporate Identification Number: U40300DL2019PTC347872	India	Water and waste management activities	1. Ankit Srivastava 2. Neha Srivastava
2020	12418002 Canada Inc. (Dissolved) Corporation Number: 12418002	Canada	Not known	2. Neha Srivastava

Annexure-III

Sample of Google AdSense Accounts Generating Income for the Srivastava Group Forums

	Adsense/ Publisher ID	Analytics ID	Domains Embedded	Estimated Monthly Revenue*
1.	pub-3981238406306300	ua-179141944	euoutlook.com	\$3,480
2.		ua-176020173	hamarahind.com	\$44,160
3.		ua-179123545	naidillitimes.com	\$5,490
4.		-	newdelhitimes.com	\$3,480
5.	-	ua-63370221	sadf.eu (Anti-Pakistan forum led by Paulo Casaca)	\$840
6.			archumankind.com	Irrelevant
7.			cases.pt	Irrelevant
8.			e-social.pt	Irrelevant
9.			heasy.pt	Irrelevant
10.			herculano.pt	Irrelevant
11.			popularjump.com	Irrelevant
12.			portugalgolfislands.com	Irrelevant
13.			ricardoquaresma.net	Irrelevant
14.			scubdadingmadeira.com	Irrelevant

*Based on an estimated review by WorthOfWeb.com based on an open-source investigation by the author

Financial versus PR Benefits of the ‘Indian Chronicles’ for the Srivastava Family

Note:

- ‘Financial Benefits’ refers to the direct monetary opportunities available for the Srivastava Group
- ‘PR Benefits’ for the Srivastava family refers to the interests in their own name (to determine market value capitalisation)

Aspect*	Financial Benefits	PR Benefits
Behaviour		
Lobbying MEPs	No	No
Setting up dubious think tanks	No	No
Reviving UN HRC NGOs	No	No
Setting up local fake media	Yes	No
Content		
Op-Eds, written parliamentary questions, individual statements	No	No
Visits/ Events/ Demonstrations	No	No
Speaking slots at the UN	No	No

*Extracted from the ABCD Pyramid in the EU DisinfoLab’s report