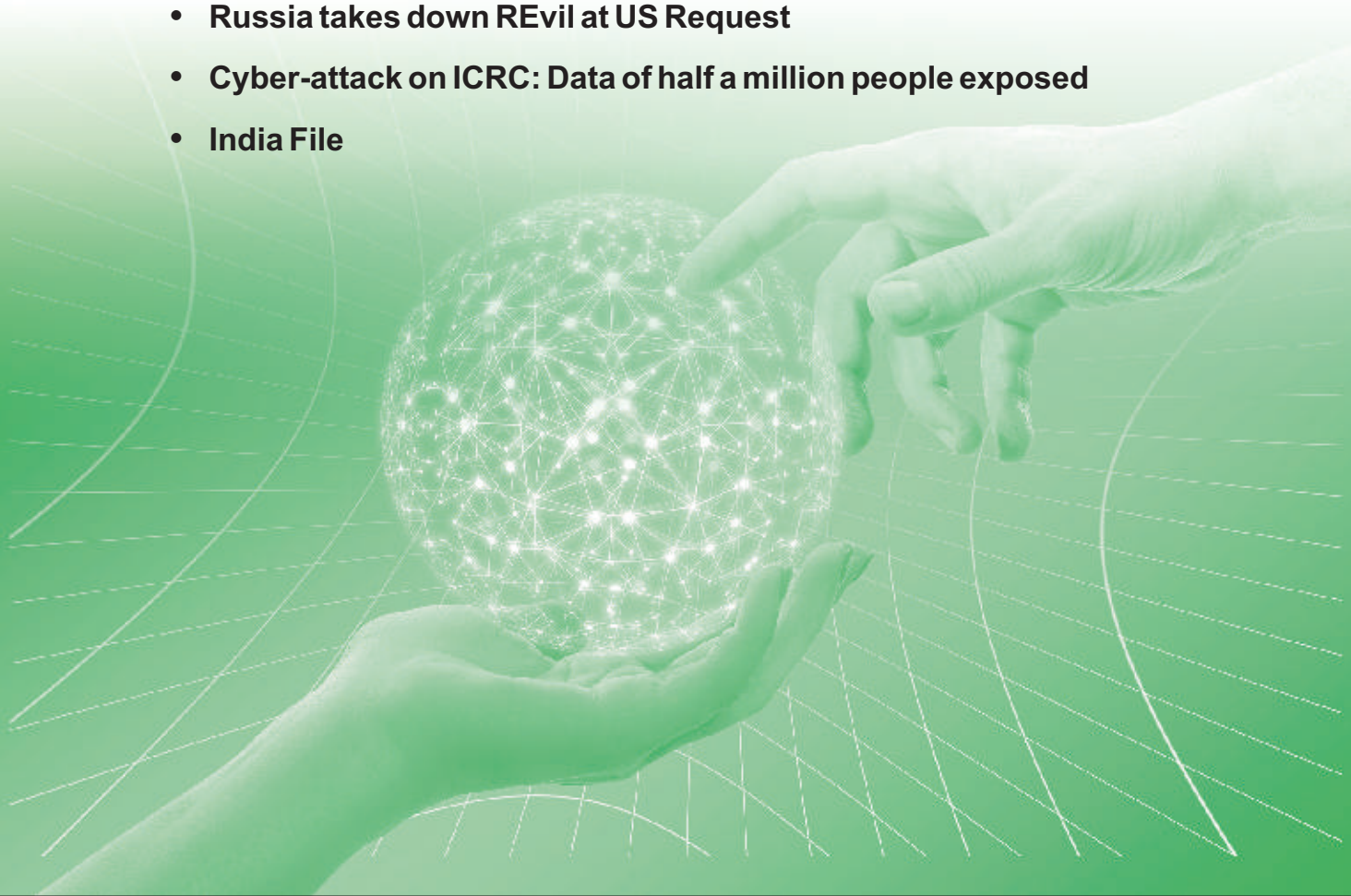
MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

# CYBER *Digest*

**February 2022**

- **WEF's Global Risks Report 2022 highlights Cyber Vulnerabilities**
- **Cyber Strategy in the National Security Policy of Pakistan**
- **WhisperGate cyber-attack on Ukrainian government websites**
- **Russia takes down REvil at US Request**
- **Cyber-attack on ICRC: Data of half a million people exposed**
- **India File**



## WEF's Global Risks Report 2022 highlights Cyber Vulnerabilities

The 2022 edition of the World Economic Forum's Global Risks Report highlights digital dependencies and cyber vulnerabilities as one of the major threats in the world today. The 17th edition of the report was compiled on the basis of views from around 12,000 country-level leaders from 124 countries who participated in its Executive Opinion Survey and Global Risks Perception Survey (GRPS). Environmental risks, debt crises, geoeconomics confrontations, digital inequalities, and cybersecurity failures are some of the biggest threats to the world, according to the report. The Covid-19 pandemic has intensified the dependence on digital systems and "cyber failure is one of the risks that worsened the most through Covid-19." There was also a 435% increase in ransomware attacks in this period.

The report noted that the decentralised Internet 3.0 would 'create a more complex threat landscape and a growing number of critical failure points'. Additionally, technologies like artificial intelligence (AI), Internet of Things (IoT)/ Internet of Robotic Things-enabled devices, edge computing, blockchain, and 5G would provide enormous opportunities to businesses with a US$ 800 billion estimated growth in value of digital commerce by 2024. On the flip side, this would also 'expose users to elevated and more pernicious forms of digital and cyber risk'. The reliance on third-party platforms for services would also pose a challenge for data privacy. The use of ransomware on 'vulnerable targets, impacting public utilities, healthcare systems and data-rich companies', spyware 'against journalists and civil rights activists across geographies', and deepfake technology to 'proliferate disinformation and wreck societal havoc' would also be exacerbated. There was an urgent need for 3 million cyber professionals worldwide to help in mitigating these risks.[1]

## Cyber Strategy in the National Security Policy of Pakistan

Pakistan released its first ever National Security Policy on 14th January 2022. The policy aims to focus on a non-traditional security approach that focuses on a citizen-centric framework instead of a one-dimensional security policy based on the development of military capabilities.[2] In terms of Pakistan's strategy on cyber, the report contains three related sections, namely: 1) Information and Cyber Security Threats, 2) Hybrid Warfare, 3) Space, Information and Security. The document considers the cyber and space domains along with land, air, and sea important for territorial integrity which can be achieved by 'defence, deterrence, astute diplomacy, and the building of robust space and cyber capabilities'. In terms of maritime security, Pakistan is worried about 'cyber intrusion and surveillance of sea lines of communication along the Indian Ocean'.

The 'Information and Cyber Security Threats' section discusses the importance of instituting robust mechanisms to protect cyberspace, investments in cyber security of critical infrastructure, and building domestic capacity to monitor and minimise both surveillance and cyber intrusion. In the 'Hybrid Warfare' section, the policy states that hybrid warfare tools include 'information and cyber warfare, disinformation, influence operations, lawfare, and economic coercion' and to counter these threats, Pakistan will adopt a 'holistic, interconnected whole-of-nation'

approach. In the 'Space, Information and Cyber Security' section, the emphasis is on 'combating disinformation and influence operations while enhancing information and cyber security, data security, and surveillance capacity'.[3] Overall, the flaws in the cyber section of the strategy are similar to those that have bedeviled cybersecurity strategies of other countries; too much vagueness, lack of a robust timeline for implementation, and difficulty in formulating the core cyber issues for the country.

## WhisperGate cyber-attack on Ukrainian government websites

Ukraine was hit by a gigantic cyber-attack in the second week of January, which took down multiple Ukrainian government websites, especially the Ministry of Foreign Affairs and Education Ministry. The hacked websites displayed the message, "Ukrainians! … All information about you has become public. Be afraid and expect worse. It's your past, present and future." Ukrainian officials have blamed Russia and Belarus for this attack.[4] The mode of operation for this attack seems to be similar to cyber-attacks in the 2008 Georgian conflict and 2014 Crimean peninsula annexation.[5]

The detection of malware that took down websites was first reported by Microsoft in their blog where they named the malware as 'WhisperGate'. The malware masquerades as ransomware in that a fake ransom note appears demanding $10,000 worth bitcoin to restore the user's hard drive when it is activated.[6] In actuality, the malware would already have erased all the data on the computer as soon as it was activated.

With increasing friction between Ukraine and Russia, the North Atlantic Treaty Organisation (NATO) also signed an agreement to enhance cyber cooperation with Ukraine which will give access to NATO's malware information sharing platform.[7] According to Ukrainian official figures, around 288,000 cyber-attacks took place in Ukraine in the first 10 months of 2021.[8]

## Russia takes down REvil on US Request

The Russian domestic security service, FSB, on 21st January 2022 stated that they have arrested several members of the REvil, a notorious hacking group. The FSB 'seized 426 million rubles ($5.6 million) in a raid against 14 members of the group, along with more than $600,000 worth of cryptocurrency and 20 luxury cars'. Russian officials specified that REvil was dismantled at USA's behest.[9]

The criminal hacking group had attacked around 140 organisations in 2020 and 360 organisations in 2021. They employed ransomware-as-a-service model and their victims included Jack Daniels' maker Brown Forman, forex company Travelex, law firm Grubman Shire Meiselas & Sacks, sixth-largest computer maker Acer, Apple's Taiwanese supplier Quanta, the world's largest processed meat supplier JBS Foods, IT vendor Kaseya which impacted 1,500 organizations globally, and Sol Oriens, a U.S. Department of Energy subcontractor for nuclear weapons consulting. But it was the most severe cyber-attack that took down Colonial Pipeline and crippled fuel supplies to the U.S. East Coast for several days that propelled the US government to take strict action against REvil. The Biden administration asserted that REvil is a threat to US's national security during the 2021 Russia-United States Summit in June

to President Vladimir Putin. The G7 countries too have put pressure on Russia to take action against 'transnational criminal enterprises' like REvil.[10]

## Cyber-attack on ICRC: Data of half a million people exposed

The International Committee of the Red Cross (ICRC) on 18 January informed that the servers hosting personal data of 515,000 people were compromised due to a cyber-attack. The breach included personal data like names, location, and contact information mainly of missing people and their families, unaccompanied or separated children, detainees and other people affected by armed conflict, natural disasters or migration. Furthermore, login and password details of 2,000 Red Cross and Red Crescent staff and volunteers was also compromised. According to the ICRC, "This attack has violated that safe digital humanitarian space in every way".

This breach was detected when ICRC's cyber partners detected abnormalities in ICRC servers which were subsequently taken offline before any further damage could be done. The servers contained data on the Red Cross and Red Crescent Movement's Restoring Family Links services which facilitates tracking and tracing of people separated by war, violence, migration and other causes. Such data could be misused, by States, non-state groups, or individuals to contact or find people to cause harm. There is still no clarity on who was behind this attack. [11]

## The India File

- **India-US Homeland Security Dialogue**

The Senior Officers Meeting of the India-US Homeland Security Dialogue was held on 12th January 2022. The meeting was co-chaired by the Home Secretary, Government of India, Shri Ajay Bhalla and Under Secretary for Strategy, Policy and Plans, Department of Homeland Security, Government of USA, Mr Robert Silvers. The dialogue 'reviewed the ongoing cooperation' and discussed the steps required for advancing cooperation in 'counter-terrorism, **cyber security, securing critical infrastructure and global supply chains**, maritime security, aviation security, customs enforcement and trade security' issues. Later this year, both countries will hold a Ministerial-level Homeland Security Dialogue.[12]

The first Homeland Security Dialogue between the two countries was held in 2011 when Janet Napolitano, Barack Obama's DHS Secretary visited New Delhi for discussions with former Home Minister P Chidambaram. The dialogue was re-established after discussions between India's Ambassador to the United States, Taranjit Singh Sandhu, and Secretary of Homeland Security Alejandro N. Mayorkas. The US Department of Homeland Security (DHS) announced that "Secretary Mayorkas and Ambassador Sandhu agreed to re-establish the U.S.-India Homeland Security Dialogue and to discuss important issues such as cybersecurity, emerging technology and addressing violent extremism," [13]

- **NSCS conducts First Colombo Security Conclave Virtual Workshop**

The National Security Council Secretariat (NSCS) in association with National Forensics Science University and Secretariat of the Colombo Security Conclave conducted the first Colombo Security Conclave Virtual Workshop on "**Developing Regional Cyber Security**

**Capabilities on Defensive operations, Deep/Dark Web handling and Digital Forensics**" from 10th to 11th January 2022. Delegates from Sri Lanka, Maldives, India, Mauritius, Seychelles, and Bangladesh participated in the workshop which addressed key areas of Deep Web and Dark Net Investigation and Challenges, Digital Forensics, Cyber Threat intelligence, and Defensive Operations in Cyber Domain. The workshop follows on the 5th Deputy NSA Level Meeting of the Colombo Security Conclave held on the 4th August 2021 where Members and Observer States had agreed on four pillars of cooperation including Maritime Safety and Security, Terrorism and Radicalization, Trafficking and Organized Crime and Cyber Security and Protection of Critical Infrastructure. [14]

- **India's Cyber Security Industry Revenue Doubled in 2021**

According to a report titled "India Cybersecurity Industry- Services and Product Growth Story" by the Data Security Council of India (DSCI), the Indian cybersecurity services industry grew from US$ 4.3 billion in 2019 to US$ 8.46 billion in 2021. Additionally, the Indian cybersecurity start-ups grew from US$ 740 million in 2019 to US$ 1.37 billion in 2021. In terms of professionals in the industry, cybersecurity service companies employ 2.18 lakhs and cyber product companies employ 27,000 employees. The report showcases that 74% of the analysed companies now leverage artificial intelligence/machine learning and cloud computing and automation is driving innovation in this sector. [15]

- **India-ASEAN Digital Work Plan 2022**

India and Association of South-East Asian Nations (ASEAN) members along with dialogue partner countries approved the India-ASEAN Digital Work Plan 2022 during the 2nd ASEAN Digital Ministers' (ADGMIN) Meeting on 28th January. ADGMIN is an annual meeting of telecom ministers of 10 ASEAN countries and dialogue partner countries—Australia, Canada, China, EU, India, Japan, Republic of Korea, New Zealand, Russia, UK and US. The work plan, envisages, *inter alia*, creating a system for combating the use of stolen and counterfeit mobile handsets, Wi-Fi access network interface for nationwide public internet, and capacity building and knowledge sharing in emerging areas in the field of information and communication technologies such as Internet of Things (IoT), 5G, advanced satellite communication, cyber forensics, etc.[16]

[1] The Global Risks Report 2022 at https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

[2] PM Imran launches Pak's first-ever National Security Policy; focuses on the flagging economy instead of military capabilities at https://indianexpress.com/article/world/pm-imran-launches-paks-first-ever-national-security-policy-focuses-on-flagging-economy-instead-of-military-capabilities-7723527/

[3] National Security Policy of Pakistan 2022-2026 at https://static.theprint.in/wp-content/uploads/2022/01/NSP.pdf

[4] EXCLUSIVE Ukraine suspects group linked to Belarus intelligence over cyberattack at https://www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15/?utm_source=pocket_rec

[5] Russia's FSB says it has taken down REvil hacker group at US request at https://www.theverge.com/2022/1/14/22883675/russia-fsb-revil-hacker-group-ransomware-us-request-fbi-doj

[6] Data of several Ukrainian government agencies is wiped in cyberattack at

https://www.washingtonpost.com/national-security/ukraine-russia-cyberattacks/2022/01/18/79590750-78a1-11ec-bf97-6eac6f77fba2_story.html

[7] NATO, Ukraine Sign Deal to 'Deepen' Cyber Cooperation at https://www.thedefensepost.com/2022/01/17/ukraine-nato-cybersecurity/

**[8]** Ukraine hit by 'massive' cyber-attack on government websites at https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers

[9] Russia's FSB says it has taken down REvil hacker group at US request at https://www.theverge.com/2022/1/14/22883675/russia-fsb-revil-hacker-group-ransomware-us-request-fbi-doj

[10] Russia's Takedown of REvil Sends Shock Waves Across the Cybercriminal Community at https://www.toolbox.com/it-security/security-general/news/revil-takedown-leaves-cybercriminals-in-shock/

**[11]** Cyber-attack on ICRC: What we know at https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

[12] Senior Officers Meeting of India-US Homeland Security Dialogue held today at https://pib.gov.in/PressReleasePage.aspx?PRID=1789437

**[13]** India, US agree to re-establish Homeland Security Dialogue at https://www.thehindu.com/news/national/india-us-agree-to-re-establish-homeland-security-dialogue/article34150411.ece

[14] National Security Council Secretariat-First Colombo Security Conclave Virtual Workshop on Developing Regional Cyber Security Capabilities on Defensive operations, Deep/Dark web handling and Digital Forensics at https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1789124

[15] India Cybersecurity Industry- Services and Product Growth Story at https://www.dsci.in/content/india-cybersecurity-industry-2021

**[16]** India, ASEAN approve digital work plan to combat use of stolen mobile handsets at https://www.thehindu.com/business/Industry/india-asean-approve-digital-work-plan-to-combat-use-of-stolen-mobile-handsets/article38344167.ece