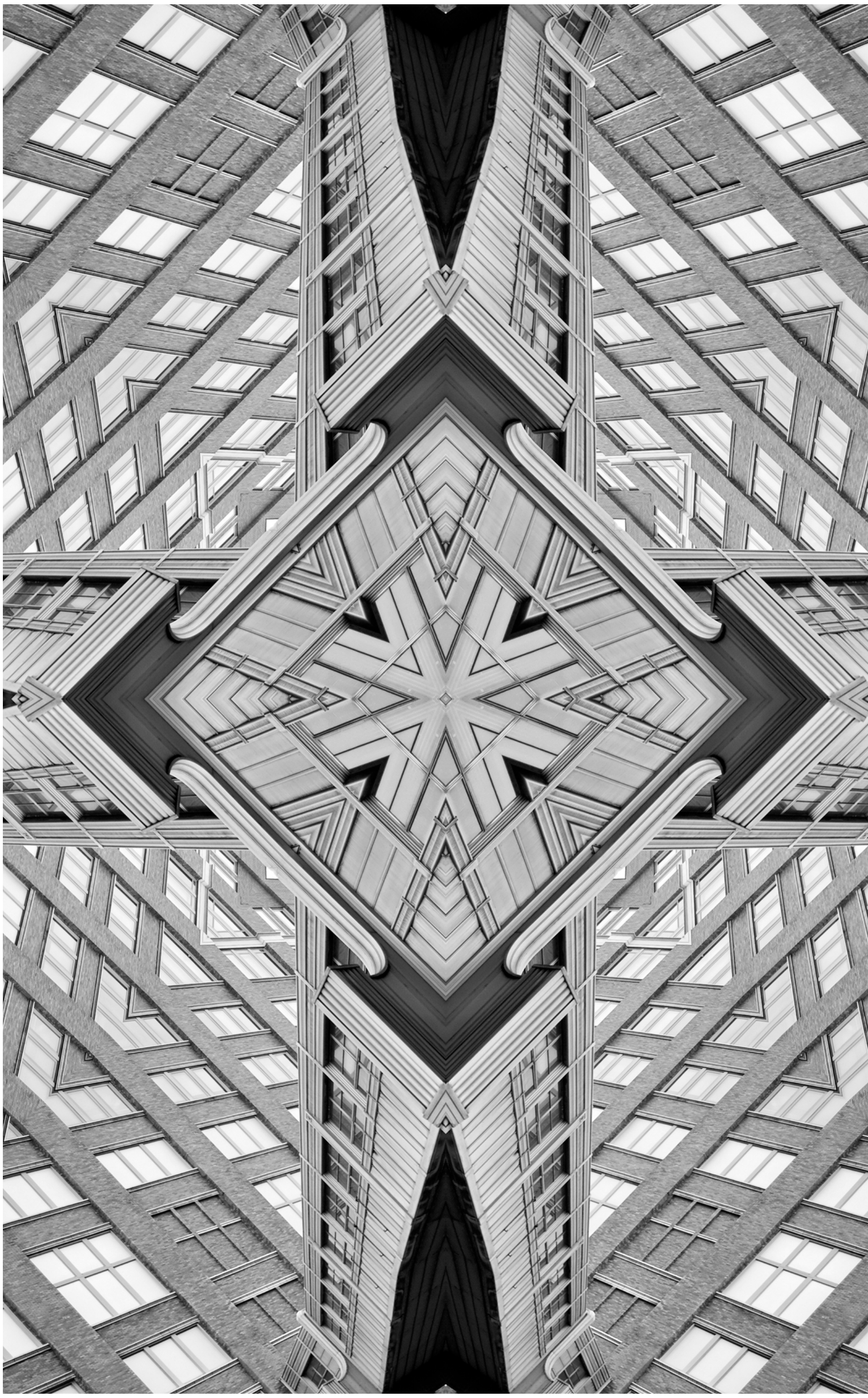
Issue Brief

ISSUE NO. 686
JANUARY 2024



Decoding the Biden Administration's Cyber Security Policy

Vivek Mishra and Sameer Patil

Abstract

The Biden administration is seeking to establish a comprehensive cybersecurity strategy as part of its national security. This issue brief analyses the US's cyber threat landscape and examines the Biden administration's cybersecurity strategy. It explores the strategy's ideological, geopolitical, technological, and diplomatic significance in a rapidly shifting domain.

Attribution: Vivek Mishra and Sameer Patil, "Decoding the Biden Administration's Cyber Security Policy," *ORF Issue Brief No. 686*, January 2024, Observer Research Foundation.

Introduction

In an era where digital connectivity propels innovation, drives economic growth, and binds national security to a vulnerable core, US President Joe Biden's administration has positioned cybersecurity at the forefront of its policy agenda. With an evolving landscape of cyber threats and an increasingly interconnected digital ecosystem, the Biden administration's approach represents a crucial response to the challenges that the US currently faces. This brief provides an overview of the US's cyber threat landscape and evaluates the Biden administration's National Cybersecurity Strategy, which was announced in March 2023.

The US cybersecurity ecosystem operates on a delicate balance between privacy and security. For the Democratic Party, which is currently in power, upholding privacy rights is critical. At times, such compulsions have run against national security imperatives, with the intelligence community's reach into private sector networks intentionally limited to safeguard individual privacy.[1] Notably, even within federal networks, the prevailing culture of limited reach and organisational constraints have hindered the intelligence community's assessment of potential threats. These limitations have led the Biden administration to push for collaborations among government agencies, the private sector, and international partners to address cyber threats comprehensively. However, in an evolving landscape of cyber threats, striking the proper equilibrium between privacy and security will be pivotal for US cybersecurity.

The US Cyber Threat Scenario

In recent years, the interconnectedness of the digital ecosystem has given rise to a host of cyber threats worldwide. Many recent cyberattacks in the US have targeted critical national infrastructure.[2] The US has experienced significant cyber incidents—such as distributed denial-of-service (DDoS) attacks[a] (targeting the country's critical national infrastructure),[3] ransomware attacks,[b,4] supply chain breaches,[c,5] zero-day attacks,[d,6] and cyber-enabled espionage campaigns[e]—that can be attributed to a range of actors, including nation-states, cybercriminal organisations, 'hacktivists', and insiders. Adversaries have repeatedly exploited the weaknesses in US servers for financial gain, espionage, disruption, and data theft. The 2014 Sony Pictures hack attributed to North Korea-backed Lazarus Group, the 2015 breach of the US Office of Personnel Management data, and the 2016 interference in the US presidential election (allegedly by Russian hackers) have highlighted the vulnerabilities in the US's cyber defence. The steady uptick in cyber incidents under the Biden administration (see Table 1) has further heightened the American threat perception in cyberspace.

Table 1: Major cyberattacks targeting the US during the Biden Presidency (2021-2023)

Month and Year	Target	Incident	Nature of Attack/ Implications
July 2023	State Department and Department of Commerce	Chinese hackers collected emails from various US government officials through a vulnerability in Microsoft's email system.	Buying and selling of critical personal data of US government officials
June 2023	Two federal agencies (Department of Energy and another whose details were not provided)	Russian-linked hackers launched a global cyberattack by exploiting a vulnerability in software commonly used by US federal agencies.	Left critical energy facilities vulnerable to alien attacks and shutdown.

[a] DDoS attacks overwhelm a target's online services by flooding them with traffic, disrupting their accessibility, and rendering them inaccessible to legitimate users, often orchestrated by a network of compromised devices.

[b] Ransomware encrypts a victim's data, demanding payment for decryption. It cripples systems, leading to data loss or disruption, with attackers extorting money in exchange for restoring access.

[c] Supply chain breaches infiltrate interconnected networks by compromising a third-party vendor or supplier, exploiting trust to access larger, more secure systems, potentially causing widespread damage.

[d] Zero-day attacks exploit software vulnerabilities unknown to developers or vendors, providing attackers an edge by launching attacks before a fix or defence is available, posing severe security threats.

[e] Cyber-enabled espionage campaigns involve hacking into systems to gather sensitive information for political, economic, or strategic advantage, and are often conducted by state-sponsored groups or advanced persistent threats, aiming for long-term access and intelligence gathering.

The US Cyber Threat Scenario

Month and Year	Target	Incident	Nature of Attack/ Implications
June 2023	Hospital in Illinois	The hospital became the first health facility to cite a ransomware attack as the main reason for closing its doors.	The cyberattack caused irreversible damage to the hospital's finances, leading to its closure.
May 2023	US outpost in Guam	Chinese hackers accessed communication networks at a US military outpost in Guam.	The hackers having access to legitimate credentials of US military personnel made detection harder.
April 2023	US infrastructure	Iranian state-linked hackers launched a series of attacks that targeted vital infrastructure in the US and other countries using unprecedented dropper malware that was modified for this specific purpose.	The group, believed to be active since 2014, is suspected of installing backdoors in various industry verticals. Specifics remain unknown.
March 2023	Federal agencies	Multiple attacks on US federal agencies as part of a cyber espionage campaign between November 2022 and January 2023, including by a Vietnamese espionage group.	The hacker found a vulnerability in the agency's Microsoft Internet Information Services server and installed malware, stealing the account information of those targeted.
March 2023	US-based cybersecurity research firms	North Korean hackers designed a phishing campaign against US-based cybersecurity research firms.	The campaign aimed to deliver malware for cyber espionage through planted Whatsapp backdoor downloads, gaining the personal information of thousands of users.

The US Cyber Threat Scenario

Month and Year	Target	Incident	Nature of Attack/ Implications
February 2023	North Atlantic Treaty Organization (NATO) networks	A pro-Russian hacking group launched DDoS attacks on NATO systems that handle and transmit sensitive data. The NATO site was also taken down temporarily.	The attack hindered communications between NATO headquarters and planes delivering aid after the earthquake in Turkey.
December 2022	FBI	Hackers seized the contact details of more than 80,000 members of the FBI threat information-sharing programme, InfraGard.	The stolen information was put on sale on the internet for US$50,000.
December 2022	US Government	Chinese government-backed hackers stole an estimated US$20 million in COVID-19 relief funds from the US government.	The money was stolen from small business administration loans and unemployment insurance money, only half of which could be retrieved. This disproportionately affected those in lower socioeconomic classes and added to the government's economic woes.
November 2022	US Merit Systems Protection Board	Iranian government-backed hackers attacked the US Merit Systems Protection Board, exploiting the log4 shell, a kind of remote code execution vulnerability enabling malicious actors to target servers.	Hackers installed cryptocurrency-mining software and malware to move around federal agency systems and acquire sensitive information.
November 2022	US public and private organisations	Hackers with suspected Chinese links masterminded an espionage campaign on public and private organisations in the Philippines, Europe, and the US, beginning in 2021.	The infection vector affected a range of public and private sector entities, primarily in Southeast Asia and extending to the US and Europe.

The US Cyber Threat Scenario

Month and Year	Target	Incident	Nature of Attack/ Implications
October 2022	Airports in the US	Independent hackers targeted several major airports in the US with DDoS attacks, affecting their websites.	A pro-Russian hacking group advertised the attack before it affected the websites. It rendered the websites of 14 public airports inaccessible.
October 2022	US state government websites	Pro-Russian hackers boasted their role in an attack that crashed the state government websites of Colorado, Kentucky, and Mississippi.	State governments' official websites were rendered intermittently inaccessible. The attack revealed Russian government-backed hackers' ability to deface websites and manipulate information, potentially impacting political outcomes.
October 2022	US defence companies	Multiple state-sponsored hackers were said to have had long-term access to defence companies, and thus sensitive information.	Information about national security was leaked for a substantial period without the authorities' knowledge.
June 2022	US telecommunications companies and network service providers	Chinese-backed hackers attacked major telecommunications companies and network services since at least 2020.	Breaches to telecommunication companies gave the hackers access to the personal data of private citizens and were used to exploit a wide variety of targets worldwide, including public and private sector organisations.
June 2022	Various US companies	Phishing campaign targeted US companies in the defence, software, supply chain, healthcare, and pharmaceuticals sectors.	The campaign stole Microsoft Office 365 and Outlook credentials from these companies.

Month and Year	Target	Incident	Nature of Attack/ Implications
May 2022	US companies	Chinese hacking groups stole intellectual property from US and European companies in 2019.	The breach jeopardised US research and development efforts and undermined these sectors' cybersecurity stance.
April 2022	USDC	North Korean hackers breached the decentralised finance platform Ronin Network and stole about US$540 million worth of Ethereum and US dollar-pegged stablecoin USDC.	Hackers siphoned money to a cryptocurrency mixer to hide the origin of funds.
April 2022	Businesses in energy, semiconductor, and telecom sectors	Two Iranian-linked cyber espionage groups targeted academics, activists, journalists, and other victims.	The campaign targeted activists, academics, and private companies, i.e., energy, semiconductors and telecom sectors in the US, along with several countries using phishing and social engineering techniques, which depicted Iran's persisting abilities to phish for credentials and surveillance operations.
March 2022	Satellite broadband service belonging to American company Viasat	Hackers attacked the American company Viasat and targeted satellite modems of thousands of Europeans.	The attack disrupted Internet services across Europe as well as Ukrainian military communication in the early stages of the Russian invasion.
February 2022	US defence contractors	Russian state-sponsored hackers breached several US defence contractors between January 2020 and February 2022. They mined emails and sensitive data regarding the companies' export-controlled products, proprietary information, and interactions with foreign governments.	The stolen data provided the attackers with substantial knowledge about US weapons platforms' development and deployment schedules, communication infrastructure plans, and the specific technologies utilised by the US government and military.

Month and Year	Target	Incident	Nature of Attack/ Implications
December 2021	US defence and technology firms	Chinese hackers attacked four US defence and technology firms.	Hackers tried to gain long-term access to computer systems to steal sensitive data from US companies.
November 2021	US defence contractor	Hackers breached employees' social security and driver's licence numbers by hacking a US defence contractor.	The stolen data endangered the identity of individuals and provided room for identity theft crimes.
November 2021	FBI's Law Enforcement Enterprise Portal	Hackers breached the FBI's Law Enforcement Enterprise Portal, a system used to communicate with state and local officials.	The extent of the data breach remains unclear.
October 2021	US defence technology companies	An Iran-affiliated hacking group tried to hack over 250 Office 365 accounts.	The targeted accounts were either of US or Israeli defence technology companies that focused on Persian Gulf ports of entry or maritime transportation companies with a presence in the region.
October 2021	US company	An American company revealed that the Russian Foreign Intelligence Service had launched a campaign targeting resellers and other technology service providers.	The attack impacted IT supply chains, including resellers and other technology service providers that customise, deploy and manage cloud services and other technologies on behalf of their customers in the US.

Month and Year	Target	Incident	Nature of Attack/ Implications
July 2021	US military personnel	Iranian hackers created fake Facebook accounts to pose as recruiters, journalists, and NGOs to attack US military personnel. They could access sensitive credentials that the victims submitted to phishing sites.	Breach of sensitive data could have potentially resulted in ransom demands from hackers.
June 2021	US-based customers of Microsoft, working for IT companies and government	Hackers linked to Russian intelligence installed malware on computers that opened a backdoor for hackers to access accounts and contact information.	The extent of the damages caused by the data breach was unclear.
June 2021	Sol Oriens	Russia-linked hacker group REvil attacked a government contractor working for the Department of Energy on nuclear weapons technology.	The breach exposed sensitive information about nuclear weapons.
May 2021	LineStar Integrity Services	The pipeline company was targeted by a ransomware attack along with Colonial Pipeline.	The attackers stole 70 gigabytes of internal files and put them on the darknet.
May 2021	Academia, airlines, construction, and energy companies	The FBI and Australian Cyber Security Centre sounded the alarms on a ransomware campaign (Avaddon) targeting various sectors in multiple countries.	The ransomware campaign disrupted the services of many companies.
May 2021	Colonial Pipeline	The pipeline was targeted in a ransomware attack, attributed to Darkside, a Russia-based criminal group.	The company faced disruptions in its operations and ultimately paid a ransom of US$ 5 million.

Month and Year	Target	Incident	Nature of Attack/ Implications
April 2021	US defence contractors	State-backed hackers, some affiliated with China, used a vulnerability in VPN service to attack organisations across the US and Europe, particularly US defence companies.	The US has regularly accused China of cyber-enabled commercial espionage targeting its defence contractors. This attack may have been part of this campaign.
April 2021	New York City's Metropolitan Transport Authority (MTA)	China-backed hackers attacked MTA. However, it was unsuccessful	Had the hackers been successful, they could have caused widespread disruptions.
March 2021	Medical researchers	Suspected Iranian hackers targeted medical researchers in Israel and the US to gain access to the credentials of geneticists, neurologists, and oncologists.	Personal and medical details of individuals associated with national security were stolen.
March 2021	US State Department	Alleged Russian hackers acquired thousands of emails after an attack on the US State Department's email server.	Through the breach, the hackers could access several pieces of classified information.
February 2021	Pfizer	North Korean hackers attempted to breach the computer systems of Pfizer, a pharmaceutical company.	The hackers sought to gain information about vaccines and treatments for COVID-19.
January 2021	Telecom companies, Internet service providers and hosting providers in the US	Hezbollah-linked hackers targeted telecom companies, Internet service providers and hosting providers in the US, UK, Egypt, Israel, Lebanon, Jordan, Saudi Arabia, the UAE, and Palestine.	The purpose of the attacks was intelligence gathering and data theft.

Source: Data compiled by authors from US government agencies and non-government websites, including news portals

The US Cyber Threat Scenario

Within a month of Biden assuming office in January 2021, the US faced a concerted cyberattack allegedly from Russia, compromising nine federal agencies and about 100 private sector companies.[7] As many as 18,000 entities had downloaded a malicious update, which then spread to a network of an unknown number of compromises, especially among companies in the private sector connected to the product-use network of impacted entities. The US government described these attacks as an 'advanced' and 'persistent' threat.[8] While the former referred to the sophistication of the attack and the knowledge of technology displayed in the process, the latter referred to the fact that the attacks specifically focused on the identity part of the network. Given the scope and scale of the attack on networks and information, it was treated as a distinct and isolated espionage case.

Cybersecurity threats originating from Russia and directed towards the US are a recognised and documented concern. In March 2022, Biden specifically warned against cyber threats emanating from Russia.[9] In the wake of the Russia-Ukraine conflict, there has been a noticeable uptick in the frequency and sophistication of these attacks.[10,11]

Some cyber threats against the US originate in China as well. In May 2023, the US and other partners issued a joint cyber advisory against a cyberattack by a China-based state-sponsored Volt Typhoon, which is said to have engaged in espionage and gathering information related to critical communications infrastructure. While Volt Typhoon had been active in the US since mid-2021 and primarily targeted critical national infrastructure in Guam and several other places in the US, Microsoft claimed that the entity's operation focussed on enhancing capabilities that could potentially interfere with vital communication networks connecting the US and Asia in times of future emergencies.[12] In July 2023, a malicious Chinese computer code that secretly embedded itself across networks of US power grids, communication systems, and water supplies made military systems vulnerable because they were connected to the networks.[13] Such embedded threats in the form of codes, which may be difficult to track, can compromise the country's military operations abroad in the event of conflict. Most recently, Chinese hackers forged the identities of Microsoft customers to read emails of US State Department employees.[14]

According to the Office of the Director of National Intelligence's 2023 Annual Threat Assessment, "China probably currently represents the broadest, most active and persistent cyber espionage threat to the U.S. Government and private-sector networks. China’s cyber pursuits and its industry’s export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland. . . China almost certainly can launch cyber-attacks that could disrupt critical infrastructure services within the United States of America, including those against oil and gas pipelines and rail systems.”[15]

One of the challenges the US faces is the ever-evolving nature of cyber threats, with traditional security measures unable to keep up. The emergence of advanced persistent threats and state-sponsored hacking groups that operate with significant resources and skill has added a new layer of complexity to the threat landscape. These groups often exploit zero-day vulnerabilities[f] to gain unauthorised access to systems and data.

Furthermore, the interconnectedness of digital systems and supply chains has introduced new attack vectors. Cybercriminals often target third-party vendors and partners to get to the primary target. This was evident in the SolarWinds supply chain attack of 2020, where attackers compromised a trusted software provider to gain access to numerous government and corporate networks. Such episodes highlight the need for a more holistic approach to cybersecurity that considers the entire ecosystem of interconnected systems.

Another gap in current cybersecurity measures is the rising threat of ransomware attacks. The May 2021 ransomware attack on the Colonial Pipeline—a major fuel pipeline originating in Houston, Texas, that carries gasoline and jet fuel to Southeastern parts of the US—highlighted the vulnerability of critical national infrastructure to cyberattacks from cybercriminal syndicates.[16] The attack, allegedly by Darkside (a Russia-based criminal group), disrupted fuel supplies, caused fuel shortages, and a surge in gas prices in some parts of the country. The disruption of the Colonial Pipeline was just one of many ransomware attacks targeting government agencies and businesses. The financial motivation behind ransomware attacks has led to a cycle of extortion, where attackers are incentivised to continue their activities and drive the growth of the ransomware-as-a-service[g] ecosystem.[17] The SolarWinds breach and the Colonial Pipeline incident underscore that cybersecurity is not solely a technical concern but a multidimensional challenge with far-reaching implications.

[f] Typically, a previously unknown software vulnerability.

[g] Ransomware-as-a-service operates as a business arrangement wherein affiliates pay ransomware operators to utilise and execute ransomware attacks created by the operators.

The US Cyber Threat Scenario

Indeed, the disruptive impact of cyber threats on the US economy and national security has been a foremost concern for many recent administrations. The ripple effects of cyber threats extend far beyond the digital realm of one country, reverberating through the economy and other national security-related domains. Cyberattacks can paralyse critical infrastructure, disrupt supply chains, ruin reputation, erode public trust in an election year, and compromise sensitive information. If conducted on other countries' networks, these could have vast implications for the US's external relations.

Consequently, the Biden administration has sought to establish a comprehensive cybersecurity strategy.

> In recent months, the US has experienced significant cyber incidents—such as DDoS attacks targeting the country's critical national infrastructure, ransomware attacks, supply chain breaches, zero-day attacks, and cyber-enabled espionage campaigns—attributed to a range of actors, including nation-states, cybercriminal organisations, 'hacktivists', and insiders.

The Biden Administration's Evolving Cybersecurity Focus

The interconnectedness of the digital world has rendered geographical boundaries meaningless, allowing state and non-state actors to target US interests from across the globe. Recent cyber threats against the US have highlighted the need for a more robust and proactive approach to cybersecurity, leading the Biden administration to adopt the National Cybersecurity Strategy. Indeed, the Biden administration is perhaps the first US government to recognise the importance of cybersecurity and usher in a greater alignment between its cybersecurity policies and the national security strategy.[h] Notably, it has involved the private sector in its cyber defence policies, augmented investment commitments, and initiated institutional restructuring to tackle cyber threats. For instance, when the SolarWinds supply chain attack was revealed in February 2021, immediate detection and effective response were complicated because it originated from within the US. Nonetheless, it responded decisively by launching an interagency review of the incident and proposed immediate actions to enhance cybersecurity practices, improve threat detection, and modernise federal networks.[18] In addition, US$750 million was earmarked for such responses.[19]

The US has embarked on a mission to fortify the nation's cyber defences. This entails enhancing threat detection and information sharing, fostering public-private partnerships, investing in cybersecurity education and workforce development, and imposing solid consequences on malicious actors.

- **Executive Order on Cybersecurity (May 2021)**

The sophistication and audacity of the SolarWinds attack prompted the administration to promulgate Executive Order (EO) 14028 aimed at "Improving the Nation's Cybersecurity" in May 2021.[20] Signalling a shift in the US approach to cybersecurity, the EO sought to modernise and enhance the federal government's cybersecurity practices and establish higher standards for software security across industries. It emphasised the importance of public-private collaboration, information sharing, and the adoption of best practices to mitigate cyber risks.

[h] While both the Trump and Biden administrations have treated cyber threats as a critical challenge for the US, the latter's approach aligns cybersecurity to the broader national security strategy, particularly partnering with likeminded partners on cybersecurity.

Towards this aim, it mandated the adoption of multiple security features such as multifactor authentication and encryption for protecting data, and the deployment of endpoint detection and response initiatives to support the proactive detection of cybersecurity incidents for federal government agencies. In addition, it directed the agencies to adopt 'zero-trust' architectures[i] and more secure cloud services.

The EO sought to enhance cooperation between the government and the private sector to improve security by removing barriers in information sharing (including breaches) between private entities (service providers) and the government. The existing mechanisms have inherently built contractual barriers to smooth information sharing between service providers and federal agencies such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the broader intelligence community.[21] In addition, to improve supply chain security, the EO sought to create a baseline standard for 'critical software' to be sold to the government by service providers. The EO also established a Cyber Safety Review Board with the power to convene a Cyber Unified Coordination Group in the event of a significant cyberattack. The EO looks to frame standard operating procedures for federal departments and agencies to respond to cyber breaches and vulnerabilities.[22]

- **National Cybersecurity Strategy (March 2023)**

The Biden administration's National Cybersecurity Strategy, unveiled in March 2023, identified a range of threats that demanded immediate attention.[23] These threats included ransomware attacks targeting critical national infrastructure, supply chain vulnerabilities, and state-sponsored cyber espionage. The strategy recognised that these threats could disrupt national security, economic stability, and public safety. The policy rationale behind the plan is to establish a comprehensive framework that would not only bolster defences against current threats but also position the US to pre-emptively address/counter emerging risks.

[i] Zero-trust architecture refers to a cybersecurity approach that eliminates any implicit trust and continuously validates every stage of a digital interaction.

The escalating scale and severity of cyber threats underscores the urgency of the Biden administration's new cybersecurity strategy. The traditional reactive approach to cybersecurity and the lack of cohesive regulations and standards created vulnerabilities that adversaries like Russia, China, and North Korea have repeatedly exploited.[24] The interconnected nature of critical national infrastructure, the proliferation of Internet of Things devices, and the increasing sophistication of threat actors have necessitated a timely and comprehensive response. The strategy marked a pivotal moment in the US's approach to cyber threats as it acknowledged the shortcomings of previous policies, the escalating severity of threats, and the need for a proactive, holistic, and collaborative approach to cybersecurity. Notably, the absence of unified cybersecurity standards and regulations across sectors posed a critical challenge in formulating a comprehensive strategy. As technology permeates every aspect of modern society, varying industry standards can leave vital systems and data vulnerable. The Biden administration's plan seeks to address this by promoting the development of cybersecurity standards and best practices while enhancing collaboration between government agencies and private sector entities.

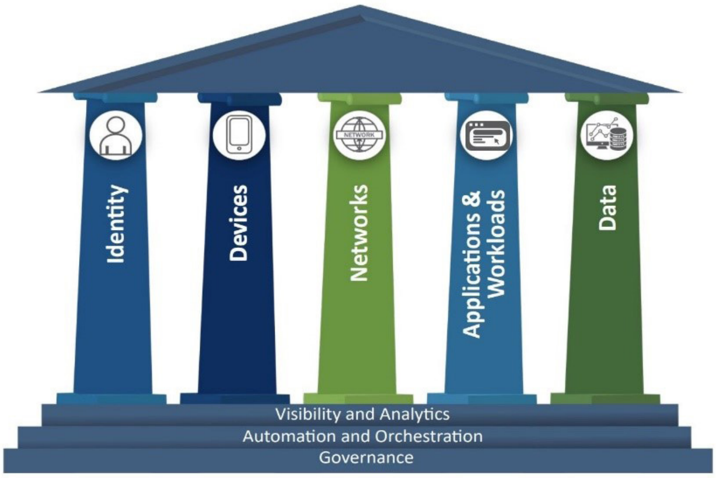
By addressing the challenges and gaps in the current cybersecurity measures, the US aims to fortify its digital defences, safeguard its critical national infrastructure, and preserve the integrity of its digital ecosystem. As the strategy is implemented, its success will depend on the collective efforts of the government, industry, and society in adapting to the evolving cyber landscape and effectively countering the multifaceted challenges that lie ahead.

- **Zero-Trust Approach**

The zero-trust approach is both a security mechanism and a value. It refers to a cybersecurity model that acknowledges that threats exist everywhere and at every level. Therefore, the only way is to authenticate and authorise every element of the cybersecurity system, including user identity, device, and location. This approach assumes that everyone and everything inside the networked system is a suspect. In a zero-trust networked architecture, the focus of security shifts from location-centric to data-centric; if the focus was previously on securing the entry points in a networked system, the focus is now on protecting the data despite its access. The erstwhile location-centric approach focused on a linear access verification model where users within a networked system would be granted access after verification of credentials and were then considered trusted entities. In most cases, no further verifications were required. The zero-trust approach puts in place a continuous cycle of validation and authorisation. This approach does not rely on the fixed perimeter of a networked system, as the boundaries keep shifting with remote usage and cloud services.[25]

As it transitions towards a zero-trust architecture, the Biden administration has created a zero-trust maturity model (ZTMM) to guide government agencies in making their computer systems more secure. The ZTMM is divided into five pillars and three cross-cutting capabilities that feed into each other in different ways to strengthen security at every level (see Figure 1).[26]

Figure 1: Zero Trust Maturity Model



Source: US Cyber and Infrastructure Security Agency[27]

- **Bipartisan Infrastructure Deal (November 2021)**

The US's current cybersecurity ecosystem is tethered to its infrastructure, energy security, technological development, and manufacturing in unprecedented ways. The Biden administration's view approach towards cybersecurity covers three aspects: first, to make cyber defence simple and wide-ranging in scope so that defending cyberspace becomes more accessible, cheaper, and more effective; second, to narrow the spectrum of cyber incidences and their impact; and third, to align its value-based approach of national security with its role safeguarding the digital world.[28]

This interconnected approach led the Biden administration to include cybersecurity in its Bipartisan Infrastructure Deal, also known as the Infrastructure Investment and Jobs Act, signed in November 2021.[29] This Act seeks to overhaul infrastructure, competitiveness, and security by investing in various interlinked sectors. An essential aspect of this Act is to ensure all Americans can access reliable high-speed internet through broadband connectivity. The legislation allocates US$65 billion to increase internet coverage to 30 million more people and lower the average cost of broadband connectivity in the US. Notably, the Infrastructure Deal links security threats to physical and natural systems by bracketing cybersecurity with the impact of factors like climate change and extreme weather events with a financial commitment of US$50 billion.

The deal also seeks to expand the scope of cybersecurity components of the law to local and state levels. To this end, the State and Local Cybersecurity Grant Program was created under the Act, which allocates US$1 billion in funding to state, local, and territorial (SLT) partners over four years. The CISA and Federal Emergency Management Agency have partnered to provide US$374.9 million in grants to SLT partners to boost cybersecurity nationwide until July 2023.[30]

- **Focus on Interagency Coordination and Institutional Interlinkages**

The Biden administration's cybersecurity approach also strengthens interagency coordination within and outside the federal government network. The basis of interagency coordination is the Trump administration's Cybersecurity and Infrastructure Security Agency Act of 2018,[31] which established the CISA under the Department of Homeland Security (DHS) as a central body to coordinate activities around cybersecurity and lead the federal government's response across the board, including threats to civilian infrastructure. The CISA is meant to be a reformed version of the National Protection and Programs Directorate,[32] formed in 2007 as a body under the DHS to reduce and eliminate threats to critical physical and cyber infrastructure. While the Trump administration's national cyber strategy established market incentives as a critical component to strengthen cybersecurity, the Biden administration's cyber security strategy seeks to embrace mandatory standards.[33]

The CISA has two leading operational roles. First, it assumes the role of the primary executor in federal cybersecurity. Its responsibility involves safeguarding and fortifying the computer networks of the federal civilian executive branch in a strong collaborative effort with the Office of Management and Budget, the Office of the National Cyber Director, and the Chief Information Officers and Chief Information Security Officers of federal agencies. Second, the CISA is the central coordinator for the security and durability of critical national infrastructure, collaborating with various governmental and industrial partners.

In March 2022, Biden enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 into law. The law is an essential step in consolidating and streamlining the CISA's position and the reporting of cyber incidents to the agency. It mandated the reporting of cyberattacks to the CISA within 72 hours of the breach and the reporting of any ransom payments within 24 hours.[34] The proposed Bureau of Cyber Statistics[35] by the Cyberspace Solarium Commission in 2020[36] is expected to complement the CIRCIA by collecting, processing, analysing, and disseminating information related to the incidents and their broader impact.

In March 2021, the DHS became critical to the Biden administration's cybersecurity approach, with the CISA as its primary organisational lead for cross-agency facilitation of safe and secure networked infrastructure, awareness, and timely responses in cybersecurity. The DHS held a 60-day cyber sprint (discussed in the subsequent section) to establish inter-agency coordination, enhance understanding, and operationalise the vision outlined in EO 14028 the following year.[37] The DHS has also established an internal working group that includes members from the CISA, the US Secret Service (USSS), and the US Coast Guard (USCG), as well as policy, legal, and Congressional experts.

As part of its multi-organisational efforts, the DHS brings together other law enforcement agencies like the USCG to protect US maritime interests from any cyberattacks; the USSS to protect US financial systems by preventing money laundering, identity theft, social engineering scams, and business email compromises; the Immigration and Customs Enforcement - Homeland Security Investigations for law enforcement in areas like the darknet and cyber-related criminal investigations; the Office of the Chief Information Officer for strong cybersecurity practices within the DHS; and the Office of Policy for leading the 'whole of government' approach to "coordinate, de-conflict, and harmonize cyber incident reporting requirements through the Cyber Incident Reporting Council."[38]

Other organisations fostering interlinkages in cybersecurity include the Cyber Safety Review Board (an independent advisory committee that is overseen by the DHS through the CISA), which assembles cybersecurity experts and public and private sector leaders to analyse and provide insights into the most significant cyber events (for example, in August 2023, the Cyber Security Review Board reviewed the malicious targeting of cloud computing environments and recommended ways to strengthen identity management and authentication in the cloud[39]); and the Transportation Security Agency (that oversees the safety and security of the transportation systems), which fosters partnerships between the public and private sectors and uses regulations to enhance cyber resilience across transportation networks (for instance, private transportation companies and authorities often partner with the DHS Cybersecurity Workforce Development Toolkit for advice on training, strategising, constructing, and progressing their cybersecurity personnel[40]).

- **Cybersecurity Sprints**

Between April 2021 and March 2022, the DHS conducted six cyber sprints to enhance existing mechanisms and practices, remove bottlenecks that have constricted past efforts, and create the scope to launch new tools when needed. Cyber sprints focus on testing specific cyber resilience in specified periods. The Ransomware sprint held between April and May 2021 highlighted the mechanisms to protect systems, especially institutional networks, from ransomware attacks.[41] The Cybersecurity Workforce sprint held between May and June 2021 aimed to create a dedicated pool of experienced workers in the cybersecurity domain by recruiting a diverse and inclusive response team within the DHS.[42]

The cyber intrusion targeting a water treatment facility in Florida and the ransomware attack on the Colonial Pipeline (both in 2021) pushed the Biden administration to establish preventive mechanisms in the industrial corridor systems across the US.[43] The Industrial Corridor Systems sprint (held between July and August 2021 and inspired by the White House Industrial Control Systems Cybersecurity Initiative[j]) aimed to do precisely this.[44] The Cybersecurity and Transportation sprint held between September and October 2021 focused

[j] Launched in July 2021 by the Biden administration, the Industrial Control Systems Cybersecurity Initiative is a voluntary partnership between the federal government and crucial infrastructure sectors to enhance the cybersecurity of these vital systems. The primary aim is to safeguard critical infrastructure by promoting the adoption of technologies and systems that enhance threat visibility, detection, warning capabilities, and response readiness for cybersecurity in essential control systems and operational technology networks. The overarching objective is to significantly increase the implementation of these technologies across prioritized critical infrastructure sectors.

on improving the cyber defence of transportation systems, including aviation, rail, pipelines, and marine transport.[45]

Election security is also a vital priority of the Biden administration's cybersecurity approach.[46] As such, the Election Security sprint was held between November 2021 and January 2022 to improve the cybersecurity of democratic institutions and infrastructure.

Additionally, the DHS has outlined four priorities towards improving cyber resilience: (1) prioritising the strength of democratic systems, which includes safeguarding the integrity of elections, electoral bodies, and related entities beyond the executive branch. (2) enhancing the security of the civilian federal government networks during recovery efforts (directing the private sector to take the lead from the federal government in planning their investments to align and augment their cybersecurity priorities and reduce future threats); (3) improving software supply chain security through risk assessment and exploring innovative technologies to enhance resilience; and (4) preparing for strategic challenges and emerging technologies, such as the development and adoption of post-quantum encryption methods.[47]

- **International Cooperation**

The inherently dynamic and interlinked nature of cyber threats necessitates some international coordination on cybersecurity. The CISA's international partnerships towards mitigating cyber risks are based on four principles: advancing operational cooperation, building partner capacity, strengthening collaboration through stakeholder engagement and outreach, and shaping the global policy ecosystem.[48]

The international dimension of US partnerships with other countries in cybersecurity primarily hinges upon threats emanating from Russia, China, North Korea, and Iran.[49] The CISA, the FBI, and the National Security Agency have partnered with their counterparts in Australia, New Zealand, the UK, and Canada to create awareness about malware attacks. In August 2023, the agencies[50] worked together to spread awareness about the Infamous Chisel malware, which enabled illicit entry to compromised devices and was engineered to examine files, track data flow, and intermittently steal confidential information from the Android devices of Ukrainian military personnel.[51]

The Biden Administration's Evolving Cybersecurity Focus

The Biden administration launched the Counter Ransomware Initiative (CRI) in October 2021 to bring together allies and partners to accelerate cooperation to counter ransomware.[52] The Initiative has set up multiple working groups focused on specific aspects of ransomware under the leadership of different countries. For instance, India heads the resilience working group,[53] the UK heads the group focused on countering the illicit use of cryptocurrency, Australia heads the group on disrupting ransomware infrastructure and actors, and Germany heads the diplomacy group.

Notably, the Biden administration has persisted with the cyber-sanctions approach imposed by previous administrations, primarily targeting Russian, Chinese, and North Korean intelligence operatives and hacking groups.[54] In April 2021, the administration gave additional powers through an EO to US government agencies to penalise Russian government agencies' interference in US elections.[55]

> "The Biden administration is perhaps the first US government to recognise the importance of cybersecurity and promote a greater alignment between its cybersecurity policies and the national security strategy. Notably, it has involved the private sector in its cyber defence policies, augmented investment commitments, and initiated institutional restructuring to tackle cyber threats."

Conclusion

The United Nations' International Telecom Union ranked the US first in its 2020 Global Cybersecurity Index[k] due to the efficacy of its legal, technical, and organisational measures, and robust capacity development efforts.[56] Notably, several key allies and partners, such as the UK, Saudi Arabia, South Korea, the UAE, Japan, Canada, France, and India, figure in the top 15 in the index, further underscoring the importance of international cybersecurity cooperation. Although the 2020 assessment precedes the Biden administration, the measures enacted since it came to power have only enhanced the US's cybersecurity approach. Still, some critics have argued that the Biden administration's cybersecurity measures are overambitious.[57] However, the impacts of many of these efforts are still emerging, impeding a concrete assessment of their efficacy.

The US cyber threat landscape continues to evolve, and adversarial actors will likely persist in their efforts to target federal agencies and American corporations to disrupt the functioning of critical national infrastructure and execute cyber espionage operations. Indeed, threats from Russia, North Korea, and China, and the competition with the latter in the military, technology, and space sectors will remain linked to the US's cyber strategy.

Vivek Mishra *is a Fellow with ORF's Strategic Studies Programme.*

Sameer Patil *is Senior Fellow at ORF's Centre for Security, Strategy and Technology, and is Deputy Director of ORF Mumbai.*

[k] The Global Cybersecurity Index (GCI) is a reliable benchmark of countries' dedication to global cybersecurity. It measures each country's level of development or engagement on five points: (i) legal measures, (ii) technical measures, (iii) organisational measures, (iv) capacity development, and (v) cooperation. A new edition of the report is currently under assessment.

Endnotes

1 Natasha G. Kohne, Michelle A. Reed, Alan Martin Hayes, Ryan Dowell, Joseph, "President Biden's AI EO: Key Takeaways for Cybersecurity & Data Privacy," *Akin*, December 1, 2023, https://www.akingump.com/en/insights/alerts/president-bidens-ai-eo-key-takeaways-for-cybersecurity-and-data-privacy

2 Adam Weinberg, "Analysis of top 11 cyber-attacks on critical infrastructure," *FirstPoint*, June 2, 2021, https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/

3 Paul Nicholson, "Five Most Famous DDoS Attacks and the Some," *A10*, January 21, 2022, https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

4 "The Latest 2023 Ransomware Statistics," *AAG*, December 1, 2023, https://aag-it.com/the-latest-ransomware-statistics/#:~:text=The%20US%2Dbased%20IC3%20received,individual%20attacks%20during%20the%20year.

5 "Annual number of entities impacted in supply chain cyber attacks in the United States from 2017 to 2022," *Statist*a, https://www.statista.com/statistics/1367208/us-annual-number-of-entities-impacted-supply-chain-attacks/

6 Anuj Mudaliar, "China-Based Hackers Exploit Barracuda Zero-Day Vulnerability to Target U.S. Government," *spiceworks*, August 30, 2023, https://www.spiceworks.com/it-security/cyber-risk-management/news/china-based-hackers-set-barracuda-zero-day-attacks/

7 The White House, *Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger,* February 17, 2021, https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/.

8 The White House, *Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger,* February 17, 2021.

9 The White House, *Statement by President Biden on our Nation's Cybersecurity*, March 21, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/.

10 Cybersecurity Infrastructure and Security Agency, *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*, March 1, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a.

11 Foreign, Commonwealth and Development Office, National Cyber Security centre, UK assesses Russian involvement in cyber-attacks on Ukraine, 18 February 2022, https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine.

12 "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," *Microsoft Threat Intelligence*, May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

Endnotes

13 David E. Sanger and Julian E. Barnes "U.S. Hunts Chinese Malware That Could Disrupt American Military Operations," July 29, 2023, *New York Times*, https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html.

14 Joseph Menn. "Chinese spies who read State Dept. email also hacked GOP congressman," *The Washington Post*, August 15, 2023, https://www.washingtonpost.com/technology/2023/08/14/microsoft-china-hack-congress/.

15 Cybersecurity and Infrastructure Security Agency, "China Cyber Threat Overview and Advisories," https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china.

16 Jen Easterly, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years," *Cybersecurity & Infrastructure Security Agency,* May 7, 2023, https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

17 Tobias Scholz & Sameer Patil. "Harnessing the G20's Potential for Global Counter-Ransomware Efforts," *ORF*, May 4, 2023, https://www.orfonline.org/research/harnessing-the-g20s-potential-for-global-counter-ransomware-efforts/.

18 Tonya Riley. "The Cybersecurity 202: Nearly two-thirds of cybersecurity experts think Biden's response to Russian hack is sufficient," *The Washington Post*, April 26, 2021, https://www.washingtonpost.com/politics/2021/04/26/cybersecurity-202-nearly-two-thirds-cybersecurity-experts-think-biden-response-russian-hack-is-sufficient/.

19 "Biden budget sets aside $750 mln for SolarWinds response," *Reuters*, May 29, 2021, https://www.reuters.com/technology/biden-budget-sets-aside-750-mln-solarwinds-response-2021-05-28/.

20 The White House, *Executive Order on Improving the Nation's Cybersecurity*, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

21 The White House, *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy*, March 02, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

22 The White House, *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy*

23 The White House, *National Cybersecurity Strategy,* March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

24 Andreas Kuehn, Debra Decker, and Kathryn Rauhut, "Whodunit in cyberspace: the rocky road from attribution to accountability," Background Paper No. 18, *ORF America*, , December 12, 2023, https://orfamerica.org/newresearch/background-cyber-whodunit

25 Eric Goldstein, "No Trust? No Problem: Maturing Towards Zero Trust Architectures," *Cyber Security and Infrastructure Security Agency*, 7 September 2021, https://www.cisa.gov/news-events/news/no-trust-no-problem-maturing-towards-zero-trust-architectures.

26 Cybersecurity and Infrastructure Security Agency, *Zero-Trust Maturity Model*, April 2023, https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf.

27 "Zero Trust Maturity Model," *Cyber and Infrastructure Security Agency, Government of the United States*, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

28 The White House, *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy.*

29 The White House, *Fact Sheet: The Bipartisan Infrastructure Deal,* November 06, 2021, HTTPS://WWW.WHITEHOUSE.GOV/BRIEFING-ROOM/STATEMENTS-RELEASES/2021/11/06/FACT-SHEET-THE-BIPARTISAN-INFRASTRUCTURE-DEAL/.

30 Jen Easterly, *CISA and FEMA Partner to Provide $374.9 Million in Grants to Bolster State and Local Cybersecurity.*

31 US Congress, Cybersecurity and infrastructure security agency act of 2018, November 16, 2018, https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf.

32 Cybersecurity Infrastructure and Security Agency, *NPDD at a glance*, https://www.cisa.gov/sites/default/files/publications/nppd-at-a-glance-bifold-02132018-508.pdf.

33 Elias Groll and Christian Vasquez, "Biden's national cybersecurity strategy advocates tech regulation, software liability reform," *Cyberscoop,* March 2, 2023, https://cyberscoop.com/biden-national-cybersecurity-strategy-2023/.

34 Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022, CISA Fact Sheet, https://www.cisa.gov/sites/default/files/publications/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf.

35 Chris Jaikaran, "Cybersecurity: Bureau of Cyber Statistics," *Congressional Research Service*, January 19, 2023, https://sgp.fas.org/crs/misc/R47389.pdf.

36 "U.S. Cyberspace Solarium Commission," July 2020, https://drive.google.com/file/d/1S5N7KvjFfxow19kCnPl0nx7Mah8pK0uG/view?pli=1

37 FY22 Cybersecurity Sprints, Department of Homeland Security, https://www.dhs.gov/cybersecurity-sprints.

38 Department of Homeland Security, Cybersecurity, https://www.dhs.gov/topics/cybersecurity.

39 Department of Homeland Security, United States Government, "Department of Homeland Security's Cyber Safety Review Board to Conduct Review on Cloud Security,"

Endnotes

August 11, 2023, https://www.dhs.gov/news/2023/08/11/department-homeland-securitys-cyber-safety-review-board-conduct-review-cloud

40 Michelle J Barns, “Transportation Systems Cybersecurity and Cyber Resilience White Paper,” *Texas A &M Transportation Institute*, https://static.tti.tamu.edu/tti.tamu.edu/documents/TTI-2023-1.pdf

41 Department of Homeland Security, DHS Actions: Cybersecurity, https://www.dhs.gov/publication/dhs-actions-cybersecurity.

42 Department of Homeland Security, DHS Actions: DHS Actions: Cybersecurity, https://www.dhs.gov/publication/dhs-actions-cybersecurity.

43 Department of Homeland Security, “DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators,” July 20, 2021, https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

44 The White House, National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

45 Department of Homeland Security, Fact Sheet: Transportation Sprint, September-October 2021, https://www.dhs.gov/sites/default/files/2022-01/dhs_transportation_sprint_fact_sheet.pdf.

46 Cybersecurity and Infrastructure Security Agency, *Election Security*, https://www.cisa.gov/topics/election-security.

47 Department of Homeland Security, *Cybersecurity,* https://www.dhs.gov/topics/cybersecurity.

48 Cybersecurity and Infrastructure Security Agency, *CISA Global*, https://www.cisa.gov/resources-tools/programs/cisa-global.

49 The White House, *National Cybersecurity Strategy,* March 2023.

50 Cybersecurity and Infrastructure Security Agency, *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure,* May 9, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a.

51 Cybersecurity Infrastructure Security Agency, *U.S. and International Partners Release Report on Russian Cyber Actors Using “Infamous Chisel” Malware*, 31 August, 2023, https://www.cisa.gov/news-events/news/us-and-international-partners-release-report-russian-cyber-actors-using-infamous-chisel-malware.

52 U.S. Department of State, *Update on the International Counter-Ransomware Initiative*, October 15, 2021, https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative.

Endnotes

53 Prashant Jha, “Grouping steps up efforts against ransomware, India a key partner,” *Hindustan Times,* November 3, 2022, https://www.hindustantimes.com/cities/delhi-news/grouping-steps-up-efforts-against-ransomware-india-a-key-partner-101667413218970.html.

54 Sameer Patil, “Assessing the Efficacy of the West’s Autonomous Cyber-Sanctions Regime and its Relevance for India,” *ORF,* September 9, 2022, https://www.orfonline.org/research/assessing-the-efficacy-of-the-wests-autonomous-cyber-sanctions-regime/.

55 The White House, FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government, April 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

56 Global Cybersecurity Index 2020, *ITU,* https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

57 Jeff Goldman, “Biden Cybersecurity Strategy: Big Ambitions, Big Obstacles,” *eSecurity Planet*, March 3, 2023, https://www.esecurityplanet.com/trends/biden-cybersecurity-strategy/

Images used in this paper are from Getty Images/Busà Photography.

ORF OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org