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

MP-IDSA
Issue Brief

The White House Executive Order on Commercial Spyware: Implications and Prospects

Rohit Kumar Sharma

May 19, 2023

Summary

The growing national security threat from misuse of commercial spyware is increasingly being recognised. The US has been taking the lead in addressing the growing menace of unregulated spyware companies and the proliferation of intrusive tools. The Biden administration's latest Executive Order relating to the issue will ensure that commercial spyware firms will be subjected to unprecedented scrutiny. Challenges though remain, including the need to persuade most states to adopt common export controls to reduce the spread of digital surveillance tools while also coordinating spyware acquisition standards across the globe.

On 27 March 2023, President Joseph Biden signed an Executive Order (EO) banning the use of commercial spyware by the United States government that poses risks to national security or has been used by foreign actors for human rights abuse.[1]The EO makes a case for the 'responsible' use of commercial spyware. It also mandates due diligence requirements on all government acquisitions through Federal Acquisition Regulations (FAR). Similarly, vendors are also required to exercise due diligence to ensure their technology is not getting used against the US' interests or for any other purposes listed in the EO.

Measures against the uncontrolled spread of commercial spyware have been in progress for a considerable duration. The EO is the latest decisive step following the series of actions by the Biden administration to deal with the proliferation of commercial spyware. Interestingly, the directive coincided with the Second Summit for Democracy, which endorsed technological advancement for democratic values and principles.[2] The US administration's lead in declaring the unregulated proliferation and misuse of commercial spyware as a national security issue will undoubtedly have positive implications, though its execution could face obstacles.

What is a Commercial Spyware?

The measures taken to prevent the misuse of spyware demonstrate an increasing apprehension towards using targeted surveillance by state and non-state actors, when done without adequate oversight or safeguard. The issue of misuse of spyware has long been in the news. International organisations have thoroughly documented the methods through which this technology has been operationalised for lawful and unlawful reasons.

Numerous terms are being used to describe the growing sector, including 'cyber mercenaries', 'intrusion as a service', 'surveillance for hire', or 'private sector offensive actors'. Using the term 'commercial spyware' is appropriate to ensure consistency throughout the text. This is particularly fitting as the term was mentioned in the EO.

According to the National Institute of Standards and Technology (NIST), spyware is defined as,

> Software that is secretly or surreptitiously installed into an information system to gather information on individuals and organizations without their knowledge.

[1] **"Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security"**, The White House, 27 March 2023.

[2] **"Declaration of the Summit for Democracy"**, U.S. Department of State, 29 March 2023.

The NIST's definition highlights the clandestine nature of gathering information without the knowledge of the target. Unlike a general explanation by the NIST, the EO shares a detailed understanding of the term 'commercial spyware', which is:

> …any end-to-end software suite that is furnished for commercial purposes, either directly or indirectly through a third party or subsidiary, that provides the user of the software suite the capability to gain remote access to a computer without the consent of the user, administrator, or owner of the computer, in order to:
>
> i. access, collect, exploit, extract, intercept, retrieve, or transmit content, including information stored on or transmitted through a computer connected to the Internet;
>
> ii. record the computer's audio calls or video calls or use the computer to record audio or video; or
>
> iii. track the location of the computer.[3]

Both definitions are similar in essence, with the only distinction being the additional details listed in the EO. The 'commercial' aspect of software suites also reflects the prevailing attitudes of the current era, wherein vendors are capitalising on the demands of buyers seeking such technologies. In fact, part of the problem is rooted in the political economy of the spyware market.

Reportedly, the need for spyware remains high from government and private clients. It is difficult to measure the scale of the industry owing to lack of transparency, although it is estimated to be worth about US$ 12 billion annually.[4] In addition, major private equity firms have provided financial support to spyware companies due to the high demand for their tools and promising business opportunities. The fact that the clients of spyware companies are largely governments is another significant factor that facilitates financial investments in these companies from equity funds.

Another significant aspect of this definition is the emphasis on the pivotal role played by third-party intermediaries and subsidiaries in facilitating transactions between vendors and buyers. This is pertinent as using third-party resellers of such technologies "complicates and obfuscates the true end-user of technology", thereby

[3] **"Executive Order on Prohibition on Use by the United States Government of Commercial Spyware"**, The White House, 27 March 2023.

[4] Ronald J. Deibert, **"The Autocrat in Your iPhone"**, *Foreign Affairs*, 12 December 2022.

creating opportunities to circumvent export control rules.[5] Also, intermediaries are crucial for vendors, particularly when they lack pre-existing relationships with individuals in the clients' acquisition departments.[6]

Foreign vendors typically rely on intermediaries based in the client's country to gain insight into the cultural intricacies that may impact their business dealings.[7] Including this aspect in the definition of commercial spyware outlined in the EO is a significant measure toward curbing the spread of such intrusive tools. In addition, Section 5(h) of the EO provides a broader interpretation of what amounts to furnishing commercial spyware. The term 'furnish' for the purpose of the order means to "develop, maintain, own, operate, manufacture, market, sell, resell, broker, lease, license, repackage, rebrand, or otherwise make available commercial spyware".

Contextualising the Executive Order

Targeted surveillance has been a longstanding practice by law enforcement agencies in combating criminal activities, preventing terrorist incidents, and aiding criminal investigation. Surveillance activities are subjected to judicial or other adequate safeguards to ensure they do not exceed legal boundaries. If left unchecked, these practices may also be used to infringe upon an individual's right to privacy. Ensuring a delicate balance between the lawful requirements of surveillance and individual privacy is challenging, especially when everything is digitally connected.

Advancement in communication technology has amplified these challenges. The ongoing tussle between government agencies and individuals and groups who seek to avoid detection perfectly exemplifies the 'cat and mouse' game. Both sides constantly evolve as they adapt and develop new strategies (in this case, technology) to gain the upper hand. It is evident that spyware companies profited out of this ongoing tussle.

While technological advancements such as encryption were seen as a boon for privacy, they also posed obstacles for law enforcement agencies. The existing surveillance tools with adequate oversight were crucial for these agencies to prevent crimes and ensure national security. Notwithstanding the range of options that state required to circumvent the encryption, including in-house capabilities or enact

[5] Miles Kenyon, **"Citizen Lab Response to the U. N. Working Group on the Use of Mercenaries"**, The Citizen Lab, 18 February 2021.

[6] Jen Roberts and Emma Schroeder, **"Makings of the Market: Seven Perspectives on Offensive Cyber Capability Proliferation"**, Atlantic Council, 1 March 2023

[7] Laurent Richard and Sandrine Rigaud, *Pegasus: The Story of the World's Most Dangerous Spyware,* Macmillan: London, 2003, p. 57.

regulations facilitating the use of legally-mandated backdoors, many governments turned to spyware companies.[8] The capabilities that were once developed by a handful of states, were now available for purchase from international private markets.

The international consortium of investigative journalists and human rights activists (The Pegasus Project), backed by forensic analysis, have extensively reported that Pegasus was considered the industry's most advanced and sophisticated spyware. Once installed, Pegasus provides unfettered access to all information on infected devices, essentially turning a smartphone into an instrument of surveillance. Taking a cue from developments, the leading spyware technology companies adjusted their focus from personal computers to cell phones, with the NSO group right out front.

It is important to note here that the commercial spyware industry extends beyond NSO including other commercial spyware vendors. Also, the Pegasus Project investigation is not the first instance of setbacks encountered by commercial spyware firms. Prior to the Pegasus scandal, Germany's FinFisher and Italy's Hacking Team held prominent positions in the market. Following the Hacking Team's massive data breach, which exposed executive emails, customer invoices and even the source code, the firm failed to recover from the episode.[9]

Despite these incidents, other commercial spyware vendors continue to provide all the components of offensive cyber operations to clients, including vulnerability research and exploits, malware, technical command and control, and employee and operational management training.[10] Seemingly, the clients perceived no harm in receiving the mix of technical, operational, and tactical capabilities to facilitate a surveillance operation.

However, with time and numerous reports drawing attention to commercial spyware being used by authoritarian regimes and other states to facilitate human rights abuses and transnational repression, the governments have begun to acknowledge the danger of such capabilities. The US has been taking the lead in addressing the growing menace of unregulated spyware companies and the proliferation of intrusive tools. Interestingly, the first major step in the US came from the Department of Commerce's Bureau of Industry and Security (BIS).

---

[8] Miles Kenyon, **"Citizen Lab Response to the U.N Working Group on the Use of Mercenaries"**, no. 5.

[9] Steven Feldstein and Brian Kot, **"Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses"**, Carnegie Endowment for International Peace, 14 March 2023.

[10] Simon Handler, **"The 5×5—Addressing the Global Market for Offensive Cyber Capabilities"**, Atlantic Council, 29 April 2022.

In November 2021, the BIS decided to add four commercial entities to the Entity list for engaging in the proliferation and misuse of cyber intrusion tools that were seen as contrary to the US's national security and foreign policy interests.[11] The U.S. Secretary of Commerce Gina M. Raimondo, released the following statement summing up the broader vision of Biden's government,

> The United States is committed to aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organizations here and abroad.[12]

Being added to the Entity List meant the companies will not be able to access American hardware and software. It was evident that the US administration seriously intended to counter such entities as the list included companies from Israel, an important US ally. For the broader public, the Department of Commerce and the Office of the Director of National Intelligence's (ODNI) National Counterintelligence and Security Center issued an advisory on practices to ensure safety from commercial surveillance tools.[13]

The growing threat from commercial spyware also figured in the Annual Threat Assessment of the U.S. Intelligence Community released by the ODNI in February 2023. The assessment highlights the growing trend among states using "spyware tools and lawful intercept programs to target criminals and terrorists" alongside using such cyber capabilities to target political opposition and dissidents.[14] Moreover, it identifies authoritarian regimes' use of commercial spyware to conduct transnational repression against individual critics and diaspora communities, including in the US and other democracies.

A week before the EO on commercial spyware, the ODNI issued binding guidance to the U.S. Intelligence Community relating to post-service employment activities of former intelligence personnel involving foreign governments and associated

[11] **"Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities"**, U.S. Department of Commerce, 3 November 2021.

[12] Ibid.

[13] **"Protect Yourself: Commercial Surveillance Tools"**, Office of the Director of National Intelligence, 7 January 2022.

[14] **"Annual Threat Assessment of the U.S. Intelligence Community"**, Office of the Director of National Intelligence, 6 February 2023.

entities.[15] The directive includes temporary and permanent restrictions. The temporary restriction prohibits post-service employment for 30 months after an intelligence community employee leaves the position. The permanent restriction applies to post-service employment on behalf of China, Russia, North Korea, Iran, Cuba, and Syria and their associated entities. However, the directive also includes provisions for providing temporary waivers of the restriction on a case-by-case basis. The directive comes against the backdrop of cases involving former US intelligence community personnel assisting authoritarian regimes in spying on journalists, dissidents, and other Americans.[16]

Executive Order on Commercial Spyware

As noted, the order was issued ahead of the second Summit for Democracy, where the US, alongside international partners, shared their intent to advance technology for democracy. The guiding principles on which the Biden administration's approach to advancing technology for democracy is predicated upon include advancing democracy and internet freedom in digital age, countering the misuse of technology and the rise of digital authoritarianism, and shaping emerging technologies to ensure respect for human rights and democratic principles.[17]

The above mentioned principles ultimately led to the issuance of the EO that limits the spread of commercial spyware and encourages the responsible use of such tools. At the outset, the order acknowledges the deployment of commercial spyware by foreign governments and persons against the US "government institutions, personnel, information and information systems". It also recognises that the same threat actors have also used commercial spyware to target political opponents, curb dissent and enable human rights abuses. Therefore, the order recognizes the need to counter and prevent the proliferation of commercial spyware for the US's national security and foreign policy interests.

The order does not completely prohibit the US agencies from using commercial spyware. Instead, it aims to prohibit the use of commercial spyware deemed unacceptable by the US government while keeping the door open to the 'responsible' use of such intrusive software. The order mandates executive departments and

[15] **"Issuance of Intelligence Community Directive 712: Requirements for Certain Employment Activities by Former Intelligence Community Employees"**, Office of the Director of National Intelligence, 23 March 2023.

[16] Joel Schectman and Christopher Bing, **"U.S. Bars Ex-Spies from Becoming 'Mercenaries,' following Reuters Series"**, *Reuters,* 17 March 2022.

[17] **"FACT SHEET: Advancing Technology for Democracy"**, The White House, 29 March 2023.

agencies[18] not to make the operational use of commercial spyware if that poses significant counterintelligence or security risks to the US or if it poses significant risks of improper use by a foreign government or person.

Actions that are deemed improper use include collecting information on individuals like activists, journalists, dissidents, political figures and others to curb dissent or enable other forms of human rights abuses. Moreover, monitoring a US person without consent to facilitate tracking and targeting the person without proper legal authorisation also corresponds to improper use of commercial spyware. The directive also outlines measures commercial spyware vendors can adopt to mitigate the likelihood of being identified as a potential risk. One such measure could involve terminating licensing agreements and contracts with clients if vendors become aware that their spyware presents the risks outlined in the EO.

To facilitate effective interagency coordination and to ensure consistency of application across the US government, the order directs information-sharing and semi-annual intelligence assessment to help agencies make informed decisions about spyware products.[19] For this purpose, the ODNI is required to issue a classified intelligence assessment on "foreign commercial spyware or foreign government or foreign person use of commercial spyware" relevant to the prohibiting factors as specified in the order. The assessment will integrate information from intelligence, open source, sanctions, and export control-related data. Before deciding to employ commercial spyware in their operations, agencies are required to conduct due diligence and notify the Assistant to the President for National Security Affairs (APNSA), explaining the due diligence completed before the decision. In addition, agencies that may make an operational use of commercial spyware are mandated to develop internal controls and oversight procedures consistent with the EO and applicable law.

Under Section 2(m) of the EO, a designated 'relevant official'[20] is empowered to grant waivers for a duration not exceeding one year of operational use of commercial spyware. Such waivers will be applicable upon the official's determination of extraordinary circumstances and the absence of any viable alternative to address such circumstances.

---

[18] **"Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security"**, The White House, 27 March 2023.

[18] Ibid.

[19] Tonya Riley, **"Executive Order Sets up Guardrails for US Use of Commercial Spyware"**, Cyberscoop, 27 March 2023.

[20] **"Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security"**, no. 18.

Furthermore, the prohibitions outlined in the EO will not apply to:

> the use of commercial spyware for purposes of testing, research, analysis, cybersecurity, or the development of countermeasures for counterintelligence or security risks, or purposes of a criminal investigation arising out of the criminal sale or use of spyware.[21]

It would be too early and unfair to appraise the efficacy of the order; however, it will undoubtedly act as a catalyst for some significant changes to come. Needless to say, the order is not a panacea to the booming industry of commercial spyware, and hence the challenges are inevitable.

Implications

The first major implication of the EO is that commercial spyware firms will be subjected to unprecedented scrutiny. Moreover, to ensure their sustainability in a market like the US, the vendors must strictly abide by the compliance outlined in the order and other existing laws. This would mean transparency in terms of former and existing clients of the vendor alongside the due diligence undertaken to ensure that the end-user is not misusing their cyber capability.

Secondly, the intelligence agencies under the supervision of the ODNI will use a classified assessment to generate a list that evaluates the level of risk associated with these companies. This process will guide federal agencies and departments in safely buying commercial spyware tools.

The order has elevated the issue of misuse of spyware to a national security issue, in letter and spirit. By doing so, it recognises that the spread of spyware is not only a domestic surveillance issue but a global threat to democratic principles. The Presidential directive also provides a robust normative framework for other countries to follow suit, morphing the issue into a global concern for countries with shared values.

The Joint Statement on efforts to counter the proliferation and misuse of commercial spyware following the second Summit for Democracy is a testament to the normative aspect of Biden's Executive Order.[22] The Joint Statement complements the EO and aims to deepen international cooperation to address the proliferation and misuse of commercial spyware. The Cybersecurity Tech Accord, an international coalition of

[21] Ibid.

[22] **"Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware"**, The White House, 30 March 2023.

private companies, also released principles to guide the technology industry to help curb the rapidly growing market of 'cyber mercenaries'.[23]

However, implementing these changes would not be without challenges. Evidently, the order only prohibits the federal agencies and closes the market to certain spyware vendors, limiting their access to the US. This would mean the state and local governments do not have the same legal obligations as federal agencies under the order. Similarly, the order is silent on financial institutions that fund these companies to accrue dividends from the sale of intrusive tools. The private equity funds and other investments remain the backbone of these commercial spyware companies. Leaving these investment firms without any legal requirements for due diligence would defeat the purpose that underlines the order.

Another major challenge would be to persuade most states to adopt common export controls to reduce the spread of digital surveillance tools while also coordinating spyware acquisition standards across the globe. The existing international regime like The Wassenaar Arrangement has clearly failed in restraining the burgeoning spyware industry. The intrusion software clauses of the Wassenaar Arrangement aimed at safeguarding activists and dissidents from government surveillance have been rendered ineffective due to the increasing instances of spyware misuse.

Given that the Wassenaar Arrangement is not a treaty and lacks formal mechanism to enforce compliance, the spyware companies operate in countries with weak regulations or enforcement mechanism. This makes it easy for these companies to develop and distribute spyware with impunity. This is pertinent as it has been reported that companies establish subsidiaries in states that are willing to overlook spyware operations and are flexible with human rights-related compliances.[24] Overall, this pioneering step by the US will undoubtedly upset the commercial spyware industry and would compel these firms to revamp their *modus-operandi* in harmony with human rights principles.

[23] **"New Industry Principles to Curb Cyber Mercenaries"**, Tech Accord, 27 March 2023.

[24] Steven Feldstein and Brian (Chun Hey) Kot, **"Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses"**, Carnegie Endowment for International Peace, 14 March 2023.

About the Author

Mr. Rohit Kumar Sharma is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses