RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg No. 042 – 26 May 2023

No. 042/2023 dated 26 May 2023

Cyberspace and American Power – The US Cybersecurity Strategy 2023

Kevin Chen Xian An

SYNOPSIS

In response to mounting concerns about cyberattacks, the Biden administration launched its National Cybersecurity Strategy on 2 March 2023. The 2023 strategy echoes numerous aspects of its predecessors but also diverges from them in significant ways. ***KEVIN CHEN XIAN AN*** *traces the evolution of these strategies to give a sense of where US strategic thought on cybersecurity is heading and how Washington increasingly views cyberspace.*

COMMENTARY

The United States has come under increasing threat from online actors in recent years. The Federal Bureau of Investigation reported that ransomware attacks, in which cybercriminals block access to a network until a sum of money is paid, affected at least 649 organisations across 14 of America's 16 critical infrastructure sectors in 2021. One such attack on Colonial Pipeline in May 2021 forced the company to temporarily shut down all its pipeline operations, resulting in widespread fuel shortages.

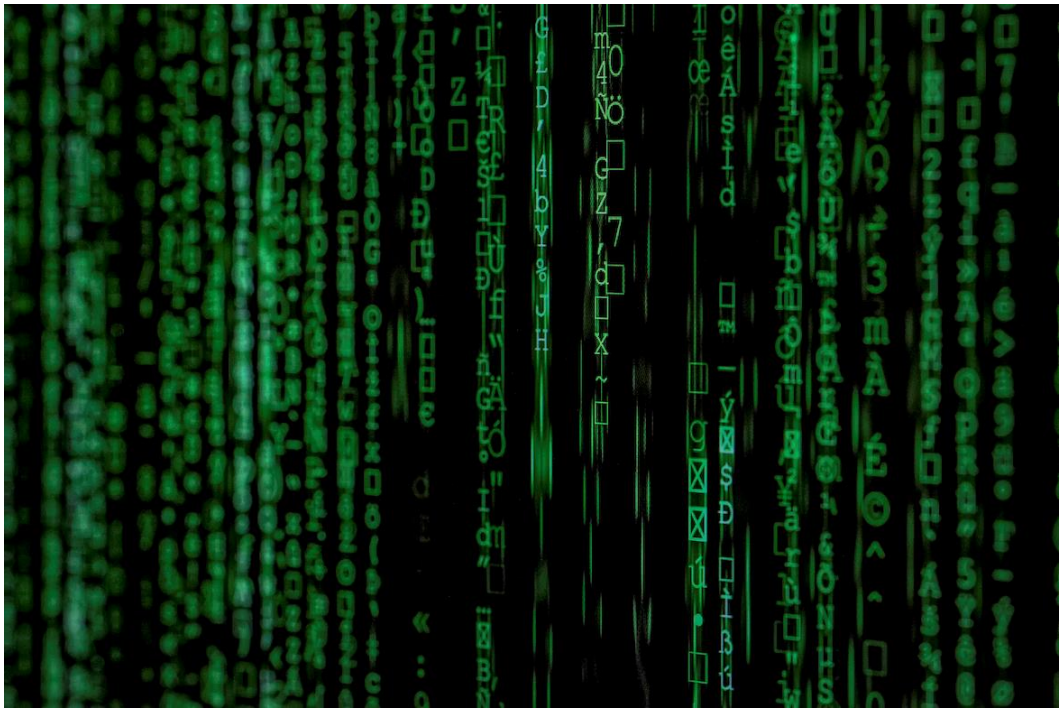
Given the rising threat of cyberattacks, the launch of the National Cybersecurity Strategy on 2 March 2023 by President Joe Biden was a welcome development. At first glance, the document shares numerous aspects with its predecessors, but observers should view these similarities – as well as differences – in context. From market-driven to government-regulated, and defensive to aggressive, the 2023 strategy is not old wine in a new bottle, but the next stage in US strategic thought.

The Evolution of US Cybersecurity Strategy

The foundation of US cybersecurity strategy is “the healthy functioning of cyberspace”, as stated in the 2003 National Strategy to Secure Cyberspace. The 2003 document cautioned that increasing digitalisation left the US economy vulnerable to cyberattacks and it sought to prevent or minimise the damage from such incidents. At the time, the Bush administration’s focus on crisis response pointed to a defensive approach to cyber incidents. Instead of an element of US national power to be applied in pursuit of national objectives, cyberspace was treated as a platform for other forms of power. Simultaneously, the strategy emphasised that the government should “lead by example”, instead of by regulation, thus allowing market forces to compel private action.

This defensive approach was discarded in the 2018 National Cyber Strategy under President Donald Trump. His strategy still called for only a limited government role, but it accused specific challengers (Russia, China, Iran, North Korea) of undermining America’s economic and political system through cyberattacks. In doing so, the 2018 strategy explicitly highlighted the political dimension of cyberattacks.

Public statements by then National Security Advisor John Bolton hinted that the political restraints surrounding retaliatory cyberattacks by the US Cyber Command were removed by the Trump administration, allowing them to undertake operations to create “structures of deterrence”. This marked the first time that discourse on cyber operations was couched in Cold War–era notions of deterrence. While doubts still persist about whether deterrence works in cyberspace, Washington clearly shifted towards a more aggressive stance on cybersecurity under Trump.



The US Cybersecurity Strategy 2023 under the Biden administration shares several similarities with previous strategies but takes on a distinctly more aggressive and government-regulated approach compared to its predecessors. *Image from Unsplash.*

The 2023 Strategy in Perspective

The 2023 strategy at the outset reads like an updated version of its predecessors. Its first pillar reiterates the need to defend critical infrastructure through features such as zero-trust principles, which institute strict authentication requirements. Its second pillar discusses ways to "disrupt and dismantle threat actors", ranging from "cyberspace operations" intended to deter attacks to "disruption campaigns" such as law enforcement efforts to render cybercrime unprofitable. Rather than downplaying the aggressiveness of the 2018 strategy, the Biden administration appears to echo its treatment of cyberspace as an element of US national power.

Differences between the two strategies become apparent in the fourth pillar, principally due to Biden's political goals. For example, both the 2018 and 2023 strategies identify supply chain risks as a concern when building new infrastructure. However, the 2023 strategy goes further to prioritise clean energy due to its importance as a key sector for US competitiveness. The 2023 strategy also makes more specific references to how cybersecurity is integrated into legislation passed under the Biden administration, including the Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act and the Inflation Reduction Act.

Under the fifth pillar, the 2023 strategy names specific mechanisms such as the Quadrilateral Security Dialogue (Quad) and Indo-Pacific Economic Framework for Prosperity (IPEF) as partnerships where the US can advance cybersecurity cooperation. By comparison, the 2018 strategy's equivalent pillar only called for cooperation with "like-minded partners" under the ominous title of "advancing American influence".

Still, the 2023 strategy stands out most in its third pillar, which eschews market forces in favour of regulatory frameworks to address cybersecurity failures. The strategy aims to reallocate the responsibility for securing cyberspace from individuals and small companies, which have limited resources, to "the biggest, most capable, and best-positioned actors" in the US digital ecosystem. Details are still emerging about how this concept of liability will be applied, but it still marks a significant departure from previous strategies.

Implications of the 2023 Strategy

The 2023 strategy's call for assigning liability for cyber failures represents a fundamental reimagining of America's cyber strategy. From defensive, market-driven beginnings, the shift towards an aggressive, regulation-driven approach to cybersecurity points to an acknowledgement that cyberspace is both an integral component of US national power and an arena that must be defended.

Legislation on liability requirements is likely to face implementation issues, including resistance from industry actors and political opposition from the Republican-controlled Congress. Still, some observers have applauded the move as a necessary measure, comparing its significance to *Grimshaw v. Ford Motor Company*, a 1978 lawsuit over safety flaws in Ford Pinto automobiles. Ford lawyers argued that their client did not intend to cause injuries to their customers, but it was ruled that Ford failed to address

a known flaw in the Pinto model. The same logic may prevail in cybersecurity if software standards are clearly defined.

For international observers, a more troubling question concerns US cyber operations. It is unclear how offensive operations will be squared with US efforts to promote norms for responsible state behaviour with its partners, especially given the challenge of ensuring cyber operations do not spiral out of control. The onus will be on US partners, including Japan and ASEAN, to discuss such matters further during platforms such as the ASEAN-US Cyber Policy Dialogue.

Kevin CHEN Xian An *is an Associate Research Fellow in the US Programme at the Institute of Defence and Strategic Studies, S. Rajaratnam School of International Studies (RSIS).*

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg