ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

CYBERSECURITY UNDER THE BIDEN ADMINISTRATION: ISSUES AND WAY FORWARD

By
Aamna Rafiq
Research Associate
Arms Control & Disarmament Centre, ISSI

Edited by
Malik Qasim Mustafa

April 24, 2021

Since January 20, 2021, the new US President, Joe Biden, has started 'erasing the legacy of the Trump administration' with the blitz of executive orders on healthcare, immigration, climate change, border wall, racism and immigration.[1] He extended the NEW START, the last remaining arms control treaty between the US and Russia after much delay by the Trump administration and negotiating to reenter the Iran Nuclear Deal. But how the Biden administration will reverse the damage being done to cybersecurity in the last four years and respond to ever-increasing cyber challenges at national and international levels are also critical issue areas to look at. President Biden in his speech at the US Department of State has promised to prioritise cybersecurity. "We've elevated the status of cyber issues within our government…. We are launching an urgent initiative to improve our capability, readiness and resilience in cyberspace,"[2] he said.

What are the key national and international cyber issues that demand significant attention? What measures President Biden has taken so far for cybersecurity? What the national and international community is expecting President Biden to do for security and strategic stability in cyberspace?

---

1 Annie Linskey, "Biden has Started Erasing Trump's Legacy. Now the Hard Part Starts," *The Hill*, February 14, 2021, https://www.washingtonpost.com/politics/biden-trump-legacy/2021/02/13/54129452-6c8b-11eb-9f80-3d7646ce1bc0_story.html.

2 Government of United States of America, White House, *Remarks by President Biden on America's Place in the World*, US Department of State Headquarters, Harry S. Truman Building, Washington, DC, February 4, 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world/.

2020 Solar Winds Operation

On April 15, 2021, the Biden administration announced diplomatic and financial sanctions against Russia. The executive order specifically states that Russia is responsible for meddling in the US elections and involved in various malicious activities in the cyber domain.[3] These sanctions are termed as the US response to the 2020 Solar Winds Hack. Although the US allegations of cyberattacks from Russia are not new but both, the Obama and Trump administrations, refrained from the retaliation of this level. So, what is different this time? According to various sources, the Solar Winds operation has crossed the red line in cyberspace. Keeping in view the sophistication, scale and scope, this attack is termed as one of the biggest cyberespionage attack known to date against the US. It has compromised the huge amount of classified data of approximately 100 private companies and 10 federal organisations. The response of this level does not come as a surprise because President Biden previously issued a clear and extensive statement on this issue and vowed to cyber secure the US. Although, the Biden administration is conducting investigations, imposing sanctions, focused on training of policymakers, joint cyber defence exercises with allies and increased coordination with the private sector, yet the precise contours of its new cybersecurity policy are deliberately not spelled out.

Splitting US CYBERCOM from NSA: Confusion Worse Confounded

The 2020 Solar Winds attack and allegations of foreign interference in the US Presidential elections have revived the most pressing as well as the confusing debate regarding the split of a dual-hat mechanism to administrate US CYBERCOM and National Security Agency (NSA). In the last few days of his administration, President Trump put forward a proposal for the split. However, this proposal could not see the light of the day due to strong resistance from the US Congress and the Solarium Commission. The dual-hat mechanism was opted at the time of CYBERCOM's establishment in 2009 to raise the new Command rather than developing a hybrid system between two institutions. In addition to providing support for intelligence and military operations in cyberspace, this mechanism enabled NSA to aid the new command in the development of the institutional framework and human resource. Many national and international experts consider this split more a question of "when" rather than "if" and the Biden administration will ultimately have to take this decision. Although, the US Congress has identified strict conditions to ensure a transparent and smooth spilt. However, the key indicators to measure the achievement of those conditions have not been

[3] United States of America, White House, *Executive Order on Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation*, White House, April 15, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/04/15/executive-order-on-blocking-property-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the-russian-federation/

identified.[4] This gap further complicates the split but at the same time gives the Biden administration a great deal of freedom, authority and time to attain a gradual and systematic headway without affecting the operational capabilities of these two organisations.

Key Infrastructures and Administrative Positions for Cybersecurity

The decisions the Trump administration had taken regarding key cybersecurity infrastructure and administrative positions would have a huge impact on where the Biden administration would start off. President Trump through an executive order in 2018 eliminated the position of a Cybersecurity Chief at the National Security Council (NSC). The new administration rectified this Himalayan blunder and replaced it with the new position of Deputy National Security Advisor for Cyber and Emerging Technologies. Another controversial decision of President Trump was the removal of the Director of Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) via a tweet. The Biden administration has yet to appoint the new CISA Director along with America's first National Cybersecurity Director - the position created under the *2021 National Defense Authorisation Act* on the recommendation of the *Cyberspace Solarium Commission*.[5] Furthermore, President Biden has put forward a US$9 billion investment plan for the Technology Modernisation Fund, partially dedicated to CISA and another $690 million entirely for CISA for congressional approval.[6] Since its establishment in 2018, CISA has become one of the top cybersecurity organisation acting as a bridge between the federal government and the private sector. CISA is also playing a central role in the 2020 Solar Winds hack investigation. If the Biden administration wants to achieve its goals in the cyber domain and enhance cross-sector cooperation then it must strengthen CISA.[7]

The Way Forward

Revising cybersecurity policies, drafting new cyber strategies and doctrines, appointing advisors for cyber and emerging technologies, restructuring institutional framework, establishing new specialised institutions and military commands, conducting cyber exercises, improving cyber hygiene, building alliances and increasing cyber awareness are all steps in the right direction. There is no doubt about the political will of the new administration to ensure the cybersecurity of the US and its readiness to pour billions of funding for it. However, the Biden administration as well as all the political and

4 Erica D. Borghard, "Time to End the Dual Hat?" Council on Foreign Relations, February 3, 2021, https://www.cfr.org/blog/time-end-dual-hat

5 Brad D. Williams, "Huge Step Forward:' Biden Taps First National Cyber Lead," Breaking Defence, April 12, 2021, https://breakingdefense.com/2021/04/huge-step-forward-biden-taps-first-national-cyber-lead/

6 Samantha Schwartz, "Biden to Nominate Obama DHS Alum as CISA Director: report," Cybersecurity Drive, January 25, 2021, https://www.cybersecuritydive.com/news/rob-silvers-cisa-biden-cybersecurity-strategy/593868/

7 Ibid.

military leadership in other states as well acknowledge the fact that strengthening national cyber defence is not enough. According to offence-defence theory, a major war could be only avoided if the defence gets an advantage over the offence.[8] Unfortunately, the speed and unique nature of cyberspace favour offence most of the time, if not always.

The 2020 Solar Winds operation and the US retaliation have also sparked a complex yet interesting debate on the legality of such malicious activities in cyberspace and their relation with the conflict escalation. Currently, there is no international treaty or convention that regulates cyber technologies and ensures responsible state behaviour in cyberspace. In the existing international law, the espionage activities are not explicitly illegal and almost every state including the US itself conducts various espionage operations against other states. However, cyberespionage is different from espionage in other domains. The 2020 Solar Winds operation is an interesting case in point where the US exercised its right of self-defence and imposed sanctions on Russia especially when the espionage operation crossed the US threshold in cyberspace without any infrastructural damage and human loss. What if it does inflict damage? What would be the US response? The cyberespionage operation could be easily redirected to inflict massive damage. Furthermore, the obtained information could be used for any type of malicious activities ranging from a cyberattack on counter-force and counter-value targets during a conflict to information warfare against state institutions and people in peacetime.

As a President-elect, Mr. Biden said that one of many approaches to cybersecurity is to work for international rules for cyberspace. After assuming office, the most important document titled "Interim National Security Strategic Guidance"[9] issued by the White House also reiterated the same position. The US aims to revive its commitment to international engagement on issues related to cybersecurity. It also calls for increasing collaboration with partners and allies to develop accountability mechanism for cyberattacks and forging new norms and agreements on cyber and emerging technologies to maintain strategic stability. Despite this positive outlook, the US has imposed sanctions on Russia and gearing up to compete with China. Only time will tell that how this stick and carrot policy will help the new administration in achieving its objectives in cyberspace.

---

8 Charles L. Glaser and Chaim Kaufmann, "What is the Offense-defense Balance and can we Measure it? (Offense, Defense, and International Politics)," *International Security 22*, no. 4 (1998): 1, https://web.stanford.edu/class/polisci211z/2.1/Glaser%20%26%20Kaufmann%20IS%201988.pdf

9 United States of America, White House, *Interim National Security Strategic Guidance,* White House, March 2021, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

