The Cybersecurity Policy Adjustment of the Trump Administration

Zhang Tengjun

Cybersecurity emerged as a popular issue during the 2016 presidential election of the United States with the successive email leak of the Democratic nominee Hillary Clinton and the Democratic National Committee.[1] Donald Trump, then the presidential nominee of the Republican Party, vowed to make cybersecurity an "immediate and top priority for my administration" if elected.[2] Since taking office, Trump has made some adjustments to the existing US cybersecurity policy under domestic pressures from various sides. The characteristics of these policy changes and the underlying dynamics are worth our observation and analysis.

Major Features of Trump's Cybersecurity Policy Adjustment

While the cybersecurity policy adjustment of the Trump administration experienced a dynamic process, it can be generalized that the concept of "America First" has been reflected both in the reinforcement of homeland cyber offensive and defensive capabilities and in the declining enthusiasm

Zhang Tengjun is Assistant Research Fellow at the Department for American Studies, China Institute of International Studies (CIIS).

[1] For relevant research, see Lu Chuanying, "International Cybersecurity Governance from the International Politics Perspective: a Case Study of the 2016 U.S. Presidential Election," *Global Review*, No.4, 2017, pp.33-48; David P. Fidler, "Transforming Election Cybersecurity," CFR Cyber Brief, May 17, 2017; Sheldon Whitehouse, Michael T. McCaul, Karen Evans and Sameer Bhalotra, "From Awareness to Action: A Cybersecurity Agenda for the 45th President," CSIS Cyber Policy Task Force Report, January 2017.

[2] Rebecca Shabad, "Donald Trump Vows to Strengthen Cybersecurity Capabilities," *CBS News*, October 3, 2016, https://www.cbsnews.com/news/donald-trump-vows-to-strengthen-cybersecurity-capabilities.

about global cybersecurity governance.

A tortuous process

Trump's cybersecurity policy adjustment is primarily manifested in three aspects, the first being the establishment of policy team. After winning the election, Trump appointed Thomas Bossert as Homeland Security Advisor to be responsible for top-level design of cybersecurity strategy. Serving as Deputy Homeland Security Advisor to President George W. Bush, Bossert has rich experience in cybersecurity. Meanwhile, Trump requested former New York mayor Rudy Giuliani to assemble a team on cybersecurity, which would provide intellectual input for the new government. Since Trump took office, a core team in charge of cybersecurity decision-making has gradually taken shape. On March 15, 2017, Rob Joyce, who once ran the National Security Agency's hacking unit-Tailored Access Operations, was appointed by Trump as Cybersecurity Coordinator on the National Security Council. Both Bossert and Joyce played a crucial role in the cybersecurity policy adjustment during the early days of the Trump administration. In addition, Trump's son-in-law and Senior Advisor Jared Kushner, who leads the newly created White House Office of American Innovation, was responsible for the information technology modernization of the federal government together with Chris Liddell, former Vice Chairman and Chief Financial Officer of General Motors, and real estate developer Reed Cordish. John Kelly, in the capacity of Secretary of Homeland Security, was in charge of the protection of critical cybersecurity infrastructure, and Defense Secretary James Mattis was tasked with developing cyber offensive and defensive capabilities. In this period, Bossert, Kelly and Mattis enjoyed relatively greater influence on cybersecurity decision-making, while Kushner was constantly troubled by his alleged involvement in the collusion with Russia to interfere in the 2016 US election. The actual sway of Giuliani was difficult to assess due to his controversial backstage role. However, Bossert and Royce successively resigned following John Bolton's taking office as National Security Advisor. The changes in personnel and consequent interruption to the existing balance of influence have brought difficulty to the coordination and implementation of cybersecurity policy.

The second aspect of Trump's adjustment is institutional re-organization. As vacancies were gradually filled, the Trump administration has accelerated the adjustment of cybersecurity decision-making structure, in which both the status of the Department of Homeland Security and the Department of Defense are elevated. With the merging of the Office of the Coordinator for Cyber Issues at the State Department, which was first established under the Obama administration, into the Bureau of Economic and Business Affairs in July 2017, the State Department's role in cybersecurity decision-making, especially in relevant international cooperation, was marginalized. On August 18 the same year, Trump announced the elevation of the US Cyber Command to one of the ten unified combatant commands of the Defense Department, with an eye to strengthening the United States' cyber operational capabilities. In May 2018, the position of the White House Cybersecurity Coordinator was abolished, adding to uncertainties of the National Security Council's role in cybersecurity decision-making.

The third approach to Trump's policy adjustment is releasing official documents, particularly presidential executive orders. Although the administration failed to introduce an earlier draft of order on cybersecurity,[3] Trump released an executive order on Strengthening Cybersecurity of Federal Networks and Critical Infrastructure based on the draft on May 11, 2017. The order highlights protection of federal networks, cybersecurity of critical infrastructure, and cybersecurity for the nation, requesting relevant authorities to conduct comprehensive risk assessment of their respective systems and submit improvement plans within a limited time.[4] This marks

[3] "The Trump Administration's Draft of the Executive Order on Cybersecurity," *The Washington Post*, https://apps.washingtonpost.com/g/documents/world/read-the-trump-administrations-draft-of-the-executive-order-on-cybersecurity/2306.

[4] The White House, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure.

the Trump administration's first systematic attempt to adjust the US cybersecurity policy. In addition, Trump announced the establishment of the American Technology Council, with an aim to transform and modernize the federal government's information technology.[5] The National Defense Authorization Act for Fiscal Year 2018, which Trump signed into law in December 2017, defines the concept of cybersecurity and stipulates the adjustment of relevant organizations and allocation of relevant resources. It is thus widely viewed as a de facto national cybersecurity strategy. In the US National Security Strategy released not long after, cybersecurity was again highlighted. In 2018, the Department of Energy and the Department of Homeland Security issued their respective cybersecurity strategies, announcing measures with regard to cybersecurity protection and risk management of energy system, government networks and critical infrastructure.[6]

Generally speaking, the Trump administration's cybersecurity policy adjustment does not break away from the strategic framework established during the Obama period. However, due to complicated and ever-changing domestic and international situation, and more particularly difficulties in integrating different mechanisms and personnel, the position and the extension of cybersecurity affairs have neither been adequately discussed within Trump's administration, making its signals sometimes confusing.

Reinforcement of cyber offensive and defensive capabilities

Homeland defense. In recent years, the frequent cyber-attacks on US government websites as well as leak of employee information and other sensitive data have drawn great public concern. Outdated hard and

[5] The White House, "Presidential Executive Order on the Establishment of the American Technology Council," May 1, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-establishment-american-technology-council.

[6] US Department of Energy, *Multiyear Plan for Energy Sector Cybersecurity*, March 2018, https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf; US Department of Homeland Security, *U.S. Department of Homeland Security Cybersecurity Strategy*, May 15, 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

software systems and unattended vulnerabilities make government networks susceptible to cyber-attacks. Given this, the Trump administration has put great emphasis on risk management, requiring federal agencies to conduct a systematic assessment of security holes and hazards in existing government networks under the guidance of the Framework for Improving Critical Infrastructure Cybersecurity, which was published by the National Institute of Standards and Technology (NIST).[7] Another focus of Trump's homeland cyber defense is critical infrastructure. In the administration's first National Security Strategy, six areas were identified as key to improving the security and resilience of critical infrastructure: national security, energy and power, banking and finance, health and safety, communications, and transportation. The administration stresses the importance to identify and prioritize risk, ensure those charged with securing critical infrastructure have the necessary authorities, information and capabilities, improve information sharing with partners, expand collaboration with the private sector, and deploy layered defenses.[8]

Capability building. Since taking office, Trump, under the principle of "Peace through Strength," has been trying to maintain the United States' unchallenged dominance in the cybersecurity arena. To strengthen cybersecurity capability building, Trump has proposed three priority actions: improve attribution, accountability, and response; enhance cyber tools and expertise, recruiting, training and retaining a workforce capable of operating across the spectrum of activity; and improve integration and agility, working with the Congress on intelligence and information sharing, planning and operations, and the development of necessary cyber tools.[9] In the budget proposal for the fiscal year 2019 published in February 2018, the Trump administration decided to invest $80 billion in information technology and

[7] The first version of the Framework for Improving Critical Infrastructure Cybersecurity was proposed by the NIST in 2014. A revised version was released following multiple discussions in January 2017, and is now still being updated. Originally aimed to provide guidance for critical infrastructure operators, it has become a widely cited reference document for the private sector due to its professionalism in risk management.

[8] The White House, *National Security Strategy of the United States of America*, December 2017, p.13.

[9] *Ibid*., p.32.

cybersecurity. The funding covers the building of cyber information systems, training of professionals and providing necessary resources to sustain the Cyber Mission Force (CMF). The 133 CMF teams established at Cyber Command are on track to be fully operational by the end of 2018.[10]

Constraints from domestic politics

Since Trump took office, he has been under constant pressures from both Democrats and Republicans, the media, the industrial community, the academic circle as well as the general public. Cybersecurity thus becomes a typical issue area constrained by domestic politics, which is manifested on three aspects.

The first aspect of constraints comes from the Capitol Hill. While Trump himself takes cybersecurity as a topic in the campaign instead of a major policy issue, the Congress, considering it as of great concern to national security, has criticized Trump many times for understating the importance of cybersecurity. In the National Defense Authorization Act for Fiscal Year 2018, the Congress, threatening to limit expenditures by the Defense Information Systems Agency in support of the White House Communication Agency, demanded the inclusion of national policy on cyberspace, cybersecurity and cyber warfare.[11] Dissatisfied with the congressional action, Trump complained, "The Congress should not hold hostage the President's ability to communicate in furtherance of the Nation's security and foreign policy."[12] On the issue of alleged Russian meddling of the US election, Trump has also disputed with the Congress, repeatedly claiming that the attacking source is not yet clear and could be any country. His reluctance to confront Vladimir Putin in his meeting with

[10] The White House, *Efficient, Effective, Accountable: An American Budget*, February 2018, p.41, https://www.whitehouse.gov/wp-content/uploads/2018/02/budget-fy2019.pdf; The White House, "Modernizing Government: 2019 Budget Fact Sheet," https://www.whitehouse.gov/wp-content/uploads/2018/02/FY19-Budget-Fact-Sheet_Modernizing-Government.pdf.

[11] The US Congress, "H.R.2810 - National Defense Authorization Act for Fiscal Year 2018," https://www.congress.gov/bill/115th-congress/house-bill/2810/text#toc-H3889C2DFE32040608D0435578BA6E014.

[12] Adam Mazmanian, "White House Unhappy with NDAA's Cyber Strategy Demand," December 12, 2017, https://defensesystems.com/articles/2017/12/14/cyber-war-strategy-pushback.aspx.

the Russian president in July 2018 drew harsh criticism from both parties in the Congress. As the investigation of Russian interference in the US election proceeds, the tit-for-tat between the Trump administration and the Congress over the cybersecurity issue would probably continue.

The second aspect of constraints is within the Trump administration. As cybersecurity increasingly becomes omnipresent involving politics, economy, military and society, almost all major government agencies have more or less jurisdiction on the issue. However, as the current cybersecurity decision-making structure is far from stable, balancing the internal relationships poses a challenge to Trump. Disputes even exist between Trump himself and his policy team. While Trump has avoided accusing Russia of interfering in the election, denouncing relevant investigations as a witch hunt and repeatedly lashing out at the judiciary and the intelligence community, the latest National Security Strategy still inexplicitly criticized Russia for intervening other countries' internal affairs through cyber means. This indicates the attempts within the government to balance Trump's ambiguous attitude toward Moscow.

The third aspect of constraints lies between the Trump administration and the domestic internet landscape. In stark contrast to his predecessor Obama, who advocated freedom of the internet, Trump, by proposing the concept of "information statecraft," has tried to reinforce the executive branch's dominant role in cyber governance. Media and internet companies are required to shoulder due responsibilities and take measures to prevent unfettered dissemination of malicious information on their platforms. On December 14, 2017, the Federal Communications Commission voted to remove the 2015 Open Internet Order, a set of regulations passed in the Obama era that established the principle of internet neutrality. This has triggered a heated discussion about the future of internet freedom. Trump has also thrown his discontent at the "chaos" of US domestic media, accusing the liberal "mainstream media" of fabricating "fake news" and attacking himself as well as his governance. Trump even called the news media as "the enemy of the American people."

The US President Donald Trump signs the National Defense Authorization Act for Fiscal Year 2019 at Fort Drum, New York on August 13. The Act allows the United States to employ "all instruments of national power," including offensive cyber capabilities, to deter and respond to foreign powers targeting US interests.

Reduced interest in global cyberspace governance

A noted characteristic of Obama's cybersecurity policy is the emphasis of cyber diplomacy and promotion of international norms on cyberspace, which is aimed to preserve the US dominant position in rules making of global cyberspace governance. Instead, the Trump administration has tried to pull the cybersecurity policy back into a domestic context, and shown reduced willingness to participate in international cyberspace governance.

Currently, Trump's position on cyberspace governance features a focus of bilateral relations and disdain for multilateralism. Since 2004, the United Nations has successively set up five groups of governmental experts on developments in the field of information and telecommunications in the context of international security(UNGGE), three of which published consensus reports and explored international norms, rules and principles applicable to cyberspace in a constructive way. The multilateral governance framework thereby established has been widely accepted. Under the Trump administration, the US attitude to the UN approach has turned from passive response in the Obama era to outright objection. Following the failure of the fifth UNGGE to reach agreement on a final report, Thomas Bossert asserted that the UN effort may not achieve the objective to implement the norms and hold accountable those who violate these norms, and "it's time to consider other approaches." He further indicated that the US would "pursue bilateral agreements when needed" and "work with smaller groups of likeminded partners to call out bad behavior and impose costs on our adversaries."[13] The Trump administration has set up bilateral working groups with Israel and the United Kingdom to discuss cybersecurity cooperation.

To address the "inaction" of the administration, Chair of the House Foreign Affairs Committee Ed Royce proposed the Cyber Diplomacy Act of 2017, demanding the State Department set up the Office of Cyberspace and the Digital Economy to reinforce its role in cyber diplomacy. As of the end of July 2018, the act had been passed by the House and expected to get approved by the Senate. Whether the bill would eventually come into effect depends on the interaction between the Trump administration and the Congress.

Increasing difficulty of China-US cyber interaction

Trump's cybersecurity policy adjustment has implicated the cyber relationship between China and the US. First, the role of the cybersecurity issue in bilateral cooperation is fading. Under the Obama administration, the issue, which once caused tensions in bilateral relations, turned out to be a highlight of cooperation following the summit between the two countries' leaders in September 2015. However, the momentum did not continue after Trump took office, who did not identify with the existing agreed-

[13] The White House, "Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017", https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017.

upon position and repeatedly found fault with China. While the Chinese government continued to stress cooperation and actively promoted the bilateral law enforcement and cybersecurity dialogue, the perception gap between the two sides on the importance of cybersecurity cooperation has caused inconsistency in bilateral exchanges, and the issue risks becoming an unstable factor again.

Second, the Trump administration has followed a clear interests-oriented approach when dealing with bilateral cyber affairs. To address dissatisfaction among domestic voters with the economic situation, Trump has held high the issue of trade fairness and tried to scapegoat China for the United States' own problems. On the consensus reached on denial of economic espionage activities, joint fight against cybercrimes and cyber terrorism, and protection of critical infrastructure, he has turned the cold shoulder. Instead, he has attempted to link the cybersecurity issue with economic and trade relations, accusing China of stealing US intellectual property on a large scale to obtain unfair competitive advantages. In August 2017, Trump launched the Section 301 investigation on the alleged violations of US intellectual property rights by Chinese enterprises and the forced technology transfer from US companies to China. In March 2018, based on the so-called findings of China's unfair trade practices, the Trump administration decided to impose a 25% tariff on $50 billion of goods imported from China, $34 billion of which took effect in July. Trump even threatened to pursue additional tariffs on another $200 billion of goods. The intensive frictions have brought major impacts to bilateral economic and trade relations. Given the long-term trend of the frictions, cybersecurity is likely to remain an important issue in bilateral dialogues.

Last, the absence of military mutual trust becomes the biggest uncertainty. Despite remarkable progress in bilateral military relations and increasing frequency of dialogues and cooperation, the exchanges on cybersecurity affairs between China and the United States are far from adequate compared with other aspects of military interactions. The mutual confidence building still lags behind, which would make the two sides more vulnerable to strategic misjudgment and even cyber conflicts. Moreover, as the increasingly intensive "cyber war" has turned the cyberspace into an arena to pursue political and military objectives, the militarization of cyberspace is more likely to trigger a China-US conflict.[14] It is thus critical for the two countries' military and cyber security to improve relevant crisis management and de-escalation mechanisms and establish confidence-building measures.[15]

Motives of Trump's Policy Adjustment

Trump's cybersecurity policy adjustment is a combined result of internal and external factors. On one hand, he has stepped up institutional and capacity building to address domestic demands for safeguarding homeland security. On the other hand, he launched competition with China based on the political consideration to preserve the United States' global dominance. The interweaving and interaction of these two interests have shaped the landscape of current policy.

Dilemma between electoral politics and government stability

Trump placed economic, health care and immigration issues at the top of his agenda early in office, with cybersecurity taking a backseat. However, in the face of successive cybercrimes and cases of personal information leakage, the mounting pressures from the public have forced the Trump administration to respond. A November 2017 Gallup public opinion survey shows that among 13 kinds of general crimes, 67% of US respondents are most worried about "having personal, credit card or financial information stolen by computer hackers."[16] The business community has also been

[14] Liu Ning and Lang Ping, "Sino-US Cybersecurity Relationship: Cooperation, Competition and Confliction," *Journal of Strategy and Decision-Making*, No.2, 2017, p.10.

[15] Lu Chuanying, "How to Handle China-US Cybersecurity Issue?" *FT Chinese*, September 19, 2016, http://www.ftchinese.com/story/001069400?page=1.

[16] RJ Reinhart, "Cybercrime Tops Americans' Crime Worries," Gallup, November 6, 2017, http://news.gallup.com/poll/221270/cybercrime-tops-americans-crime-worries.aspx.

pressuring Trump to combat economic cyber espionage, strengthen protection of intellectual property rights and safeguard the economic interests of US enterprises. There are simultaneous voices from the Congress, the strategic community and within the government to reinforce cybersecurity. In late August 2017, given that Trump has paid "insufficient attention to the growing threats to the cybersecurity of the critical systems upon which all Americans depend," eight members announced their resignation from the National Infrastructure Advisory Council, which advises the Homeland Security Department and the State Department on cybersecurity and infrastructure protection, and in fact paralyzed the organization.

The convergence of domestic interests on cybersecurity affairs forced the Trump administration to make a response. On one hand, it began to review the issue and strengthen the cybersecurity defense of federal networks and critical infrastructure. On the other hand, it started to squarely address the cyber threats to the US economic growth, social stability and national security from both state and non-state actors, with a focus on reinforcement of cyber deterrence and offensive capabilities.

However, such response is rather limited, mostly due to Trump's consideration for stability of his presidency. The continuous development of alleged Russian interference in the US election and the ongoing investigation of Russian collusion have made cybersecurity an issue that concerns the US democratic system and national security. Specifically, the investigation into allegations of Russian ties with his campaign, as a handy target for domestic anti-Trump forces, has caused the biggest ruling crisis to Trump since he took office. While Democrats are actively taking advantage of the Russian interference and collusion case and pushing for the ousting of several members in Trump's campaign and administration, even considering impeachment of the president once he was found involved, Republicans have generally refrained from blocking the investigation, instead urging Trump to impose stricter sanctions on Russia.

The Russian collusion investigation has seriously impacted Trump's policy team and directly hindered the process of domestic agenda. It has also made the US social landscape even more divided. The Trump administration are worried that an overly receptive approach toward domestic pressures on the cybersecurity issue would encroach on its political base and bring inconceivable consequences. Therefore, Trump has so far denied all the accusations, at some time even hoping to set up a joint cybersecurity unit with Russia to together combat cyber espionage.

Trump's policy has been hesitating between considerations of electoral politics and government stability. He does not want to offend his constituency, but he also tries to avoid anything that obstructs his governing. This leads to the dynamic feature of his policy at different times.

Polarization of political landscape

Since the end of the 20th century, the polarization of US politics has accelerated, with ideological disputes between the two major parties continuously deepening and malicious political fights becoming more frequent. Trump's cybersecurity policy adjustment is also first a reversal of his predecessor's doctrine. In the Trump administration's opinion, Obama's cybersecurity policy is flawed in the following aspects. First, there were no appropriate countermeasures in the face of continuous cyber attacks from allies, enemies and non-state actors. Yet the criticism is mainly driven by political considerations without much substantial meaning. Second, Obama's cyber deterrence strategy was not effective. The United States' cyber capabilities had not been adequately developed under Obama and was unable to fully deter potential adversaries' cyber activities. Third, the cyber governance framework promoted by Obama was infeasible. Based on a pragmatic mindset, Trump accused the original framework of limiting the United States' flexibility and harming national interests.

The partisan confrontation is also reflected in Trump's cybersecurity policy debate. As Trump's policy adjustment mostly appeals to anti-establishment Republicans and economic nationalists, not only has it been attacked by Democrats, part of it is also not welcomed by the Republican establishment. Rob Joyce's absence to the hearing on defending against cyber attacks, which was held by the Senate Armed Services Committee, was criticized by congressional members of both parties. John McCain, Chairman of the Committee and the most outspoken critic of Trump's cybersecurity policy, has repeatedly urged Trump to release a national cybersecurity strategy.

Dominant principle of "America First"

As the governing concept guiding Trump's domestic and foreign policies, "America First" features the priority of economy, the pursuit of "peace through strength," and a pragmatic approach. Trump's cybersecurity policy adjustment also follows the logic of "America First."

First, "America First" is in essence "domestic affairs first," which further comes down to "economy first." In terms of cybersecurity, "economy first" means improving digital infrastructure and promoting fairness and reciprocity in digital economic competition. The Trump administration repeatedly points out that the backwardness of the US digital infrastructure has impeded economic sustainability, and therefore the US must take measures to expand bandwidth, improve broadband connection, and build a reliable and secure internet. Meanwhile, given that competitors are stealing the US intellectual property through cyber economic warfare and other malicious cyber activities and causing damage to the US private sector, there is great necessity of stepping up fighting of cyber espionage.

Second, Trump pursues "peace through strength" in foreign policy, safeguarding the US national security and global interests by strengthening the military, the defense industry, the nuclear power, and capabilities in outer space, cyberspace and intelligence. Based on the principle, Trump gives special attention to cyber offensive and defensive capabilities. By budget increase, mechanism re-organization, technologic investment and personnel training, a mature defensive system for federal networks and critical infrastructure is to be established. Effective deterrence against potential adversaries would also be in place through the building of strong offensive retaliation capabilities.

Third, Trump's political calculation is driven by pragmatism. On one hand, Trump puts interests first and focuses on real gains and losses in diplomacy. The transactional mindset leads to his preference for bilateralism in dealing with cybersecurity affairs, which utilizes the United States' dominant cyber power to gain the upper hand in negotiations. On the other hand, Trump urges for a coalition of like-minded countries to improve mechanisms of information sharing and collective action. In fact, the primary objective of Trump's proposal is not to protect the US from cyber attacks through the coalition, but to use the opportunity to demand burden sharing from allies.

Return of great-power-politics thinking

As Trump wages an all-out competition against China, the rhetoric of "China Threat" is making a return, and cybersecurity is depicted as a major arena of the alleged threat. In the Trump administration's opinion, China's cybersecurity strategy and activities have challenged the United States in at least three aspects.

First, the Chinese ambition to develop into a cyber power challenges the US global dominance and its interests in China. In recent years, China has elevated cybersecurity to the level of national security, advancing its development and informatization in a coordinated manner. By accelerating the improvement of relevant mechanisms, China is also setting the new objective and strategy of building itself into a cyber power. Under the fresh vision, China has passed the cybersecurity law, released its cyberspace strategies, and regulated the domestic cyber environment. At the same time, the Chinese government has been actively participating in international governance, initiating the World Internet Conference, proposing the community of shared future in cyberspace, and pushing for governance solution under the UN framework. However, in the Trump administration's eyes, China is expanding its cyber power at such an unimaginable speed that the US dominance is at stake. China's strengthened management of the internet, localization of data and regulation on market access are all viewed by the US as challenging the existing rules and order and detrimental to the interests of US companies in China. Therefore, Trump has pressured China on many occasions to reduce government intervention, substantially relax market access and technology transfer requirements, and give "fair" treatment to US enterprises and investment.

Second, China's cyber attacks and espionage activities are harmful to the US strategic economic interests. Domestically, the US has been playing up the threat of Chinese cyber attacks, asserting that China's rapidly developing cyber offensive capability makes it able to collect military intelligence and steal corporate intellectual property and information about the government and its personnel. Given the alleged tremendous threat to national security, the US must take countermeasures. In his testimony made to the Senate Intelligence Committee, Director of National Intelligence Daniel Coats indicated that ongoing cyber activity from China continued to be identified, although at volumes significantly lower than before the bilateral US-China cyber commitments of September 2015.[17] Accusations of alleged Chinese cyber attacks and espionage are not infrequent within the Trump government.

Third, the surge of China's information and telecommunications industry has brought major impacts on relevant industries in the US. Chinese enterprises like Huawei and ZTE have long enjoyed a larger market share in many developing countries than their European and US counterparts, and are actively expanding the market in developed countries. Concerned about the situation, Trump has stepped up economic pressure, among other means, on relevant Chinese industries. For example, the Trump administration has blocked multiple investment as well as mergers and acquisitions by Chinese information and telecommunications enterprises on grounds of national security. The Committee on Foreign Investment in the US (CFIUS) has also been reformed to strengthen scrutiny of sensitive technology transfers. At the height of bilateral trade frictions, Trump issued a trade ban on ZTE, and conceded only after mediation by the Chinese government and a heavy price paid by ZTE. In the National Defense

[17] "World Threat Assessment of the US Intelligence Community," Office of the Director of National Intelligence, February 13, 2018, p.6, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

Authorization Act for Fiscal Year 2019, the Congress also imposed a ban on the use of Huawei or ZTE technologies by government agencies and other bodies that make transactions with the government. The US intelligence community even suggested the US citizens stop using products and services provided by the Chinese companies. These actions, on the pretext of safeguarding national security and personal privacy, are in fact aimed to protect domestic industries.

Conclusion

In spite of much inconsistency and ambiguity, Trump's cybersecurity policy adjustment has reflected a significant tendency to contract inward. However, the government's passive approach is unable to stop the private sector and the technology community, among other stakeholders, from participating in international governance. Under domestic pressures and given existence of external threats, cybersecurity would inevitably remain an important issue facing the Trump administration.

In the new period featuring China-US competition, the negative impacts of the cybersecurity issue on bilateral relations would be continuously on the rise, as Trump utilizes the issue to further challenge China. Given the extensive existence of disputes and lack of mutual trust on cybersecurity, it is obviously difficult for the two countries to manage their cyber relations. However, such difficulty in turn demonstrates the necessity for the two sides to continue dialogue, enhance mutual trust, dispel misgivings, build consensus and deepen pragmatic cooperation. Given the importance of cybersecurity and potential dangers of a cyber war, China and the US should jointly discuss the establishment of a crisis management mechanism. Furthermore, in the face of Trump's unreasonable pressures, China should also make full preparations and resolutely fight back against the United States' groundless provocations, to safeguard its own national security and economic interests.