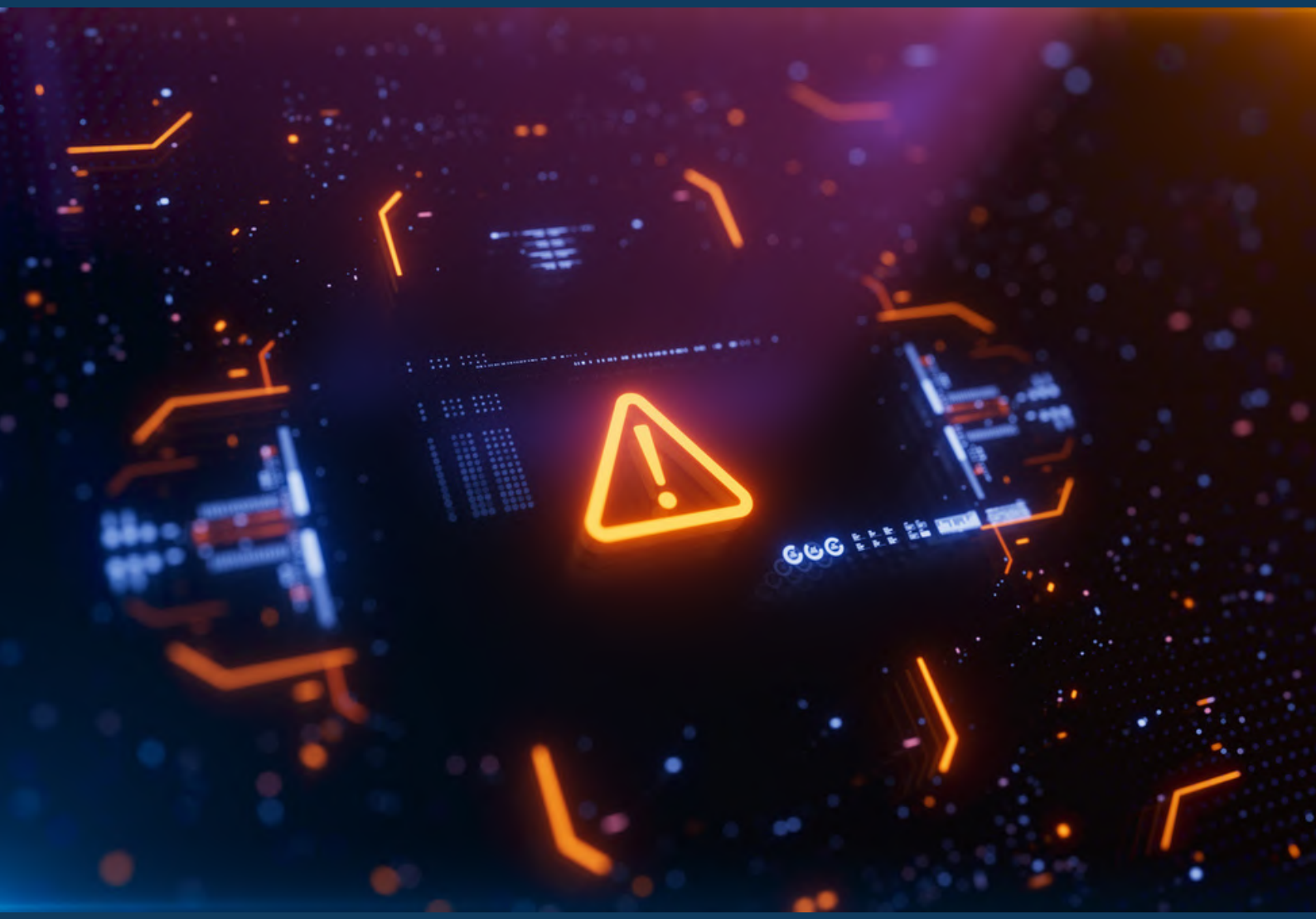
APLN

Cyber-Nuclear Nexus and Escalation Pathways

NOVEMBER 2026

FEI SU



© 2026 Fei Su

This volume is published under a 4.0 International Creative Commons License.

The views represented herein are the author's own and do not necessarily reflect the position of the Asia-Pacific Leadership Network or any of its members, board, or funders.

Please direct inquiries to: Asia-Pacific Leadership Network (APLN)
Secretariat 4th floor, 116, Pirundae-ro,
Jongno-gu, Seoul, ROK, 03035
Tel. +82-2-2135-2170
Fax. +82-70-4015-0708
Email. apln@apln.network

This publication can be downloaded at no cost at www.apln.network.

Cover Photo: iStock/amgun

CYBER-NUCLEAR NEXUS AND ESCALATION PATHWAYS

Fei Su

INTRODUCTION

The risk at the intersection of the cyber and nuclear domains has increasingly become a focal point, particularly with the continued digitalisation and automation of nuclear weapons systems and supporting infrastructure, creating vulnerabilities that can be exploited through cyber operations that infiltrate, disrupt, manipulate or disable critical functions and networks. At the same time, cyber capabilities have become increasingly sophisticated and difficult to attribute and detect, including through the growing application of artificial intelligence (AI) in cyber operations.[1]

While cyberattacks against nuclear command, control and communications (NC3) systems are perceived as being highly escalatory, cyber incidents that do not directly engage with nuclear forces can also have indirect implications for nuclear stability and generate escalation risks.[2] In particular, a growing number of cyber incidents involving critical infrastructure, such as satellite systems that perform critical functions for NC3 and early warning capabilities, as well as government agencies, research institutions and defence companies, highlight the increasing indirect cyber risks posed against nuclear capabilities.[3]

While not all cyber incidents are the result of deliberate cyberattacks (they may also result from system malfunctions or human error) an incident occurring in or around systems associated with nuclear capabilities may nevertheless initially be interpreted as an intentional cyber operation conducted by an adversary.[4] This ambiguity can complicate attribution and increase the risk of misperception, particularly when decision

[1] Lizzie Short, "AI and the Future of Cybersecurity," Harvard Extension School Blog, *Harvard Extension School*, 21 July 2025, https://extension.harvard.edu/blog/ai-and-the-future-of-cybersecurity/#Meet-Our-Experts.
[2] Wilfred Wan et al., *The Cyber-Nuclear Nexus: Interactions and Risks*, No. 2 (UNIDIR, 2021), https://unidir.org/wp-content/uploads/2023/05/NRR_CyberNuclear.pdf; Joel Petersson-Ivre and Hree P. Samudra, "APLN Membership Survey: Cyberattacks on NC3 is the greatest emerging threat," Asia-Pacific Leadership Network, April 24, 2026, https://www.apln.network/analysis/apln-membership-survey/apln-membership-survey-cyberattacks-on-nc3-is-the-greatest-emerging-threat.
[3] Larisa Saveleva Dovgal et al., *Enhancing Cyber Risk Reduction and the Role of the European Union*, (SIPRI, December 2024), https://doi.org/10.55163/XYYF1023; Lora Saalman et al., *Mapping Cyber-related Missile and Satellite Incidents and Confidence-building Measures*, SIPRI Insights on Peace and Security, No. 2023/10 (November 2023), https://doi.org/10.55163/RJMH1479.
[4] James M. Acton, "Cyber Warfare & Inadvertent Escalation," *Dædalus* 149, No.2 (2020), https://www.amacad.org/publication/daedalus/cyber-warfare-inadvertent-escalation.

makers have incomplete information with which to assess the nature and implications of a cyber incident.[5]

It is therefore important to understand the risks of cyber incidents in the nuclear domain in order to identify appropriate measures to mitigate them. This policy brief will provide a preliminary assessment of how cyber threats are perceived in nuclear doctrines, with a particular focus on China and the United States, as well as the potential escalation pathways at the intersection of the cyber and nuclear domains. It will draw on selected cases of cyber incidents that might have implications for nuclear security to examine how these dynamics play out, and how governments might respond to such incidents. It will conclude with recommendations for reducing the associated risks.

PERCEIVED THREATS

According to a survey conducted by the Asia-Pacific Leadership Network (APLN) ahead of the 2026 Review Conference of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), cyber activities targeting NC3 are perceived as highly escalatory.[6] Indeed, concerns regarding the escalation risks arising from the intersection of the cyber and nuclear domains are not new.[7] For example, there were reportedly discussions in 2021 between US President Joe Biden and Russian President Vladimir Putin on the possibility of reaching a bilateral understanding to establish a list of targets that would be off limits to offensive cyber operations during peacetime, including NC3 systems.[8] Although the establishment of explicit red lines has not been formally declared at official level, there appears to be a significant degree of convergence among experts regarding the particularly sensitive nature of cyber operations against other states' NC3 systems.[9]

The United States, for example, stated in its 2018 Nuclear Posture Review that "significant non-nuclear strategic attacks include, but are not limited to, attacks on the U.S., allied, or partner civilian population or infrastructure, and attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities."[10] The same document identified cyber aggression as one category of non-nuclear strategic threat, and raised the possibility of using nuclear weapons to respond

[5] Benjamin Brake, *Strategic Risks of Ambiguity in Cyberspace*, Contingency Planning Memorandum, No. 24 (Council on Foreign Relations, May 2015), https://www.files.ethz.ch/isn/191208/CPA_ContingencyPlanningMemo_24.pdf.
[6] Petersson-Ivre and Samudra, "APLN Membership Survey."
[7] "Addressing Cyber-Nuclear Security Threats," Nuclear Threat Initiative, accessed October 27, 2026, https://www.nti.org/about/programs-projects/project/addressing-cyber-nuclear-security-threats/.
[8] Wan et al., The Cyber-Nuclear Nexus.
[9] 'Variable 3: Preventing Nuclear War', Better Order Project, Quincy Institute, accessed October 26, 2026, https://betterorderproject.org/regulation-of-force-and-coercion/variable-3-preventing-nuclear-war/.
[10] U.S. Department of Defense, *Nuclear Posture Review* (February 2018), https://fas.org/wp-content/uploads/media/2018-Nuclear-Posture-Review-Version-2.pdf.

to a cyberattack of strategic significance.[11] Its 2022 Nuclear Posture Review likewise contains multiple references to the importance of ensuring the cyber resilience of US NC3, and expresses particular concern about the risk of inadvertent escalation arising from "unclear norms of behaviour and escalation thresholds."[12] Taken together, these statements suggest that the United States reserves the possibility of considering nuclear responses for "deterring attacks that have strategic effect" against itself or its allies and partners through "a range of non-nuclear capabilities" including from the cyber domain.[13] This appears consistent with perceptions among Chinese experts that the United States maintains a relatively expansive conception of the circumstances in which nuclear weapons could be employed.[14] In particular, China is identified by the United States as its "most persistent cyber threat" that would threaten both US NC3 and the critical national infrastructure that supports it.[15]

China's official doctrine, by contrast, does not explicitly articulate a linkage between cyber activities and the risk of nuclear use. China's 2025 White Paper on Arms Control, Disarmament, and Nonproliferation in the New Era highlights the concern over cyberattacks against critical infrastructures and its national security more broadly, while reaffirming China's No-First-Use policy.[16] It nevertheless remains ambiguous whether China would regard certain non-nuclear strategic attacks as potentially warranting a nuclear response. There are indications that China may have developed options for nuclear signalling intended to deter non-nuclear strategic attacks.[17] Such assessments have reinforced US concerns about whether China might consider "a nuclear strike in response to a nonnuclear attack threatening the viability of China's nuclear forces or C2,

[11] Jeffrey Lewis, "'WannaCry' About Trump's Nuclear Posture Review? The Global Implications of Deterring Cyber Attacks with Nuclear Weapons," Nuclear Threat Initiative, June 18, 2018, https://www.nti.org/analysis/articles/wanna-cry-about-trumps-nuclear-posture-review/.
[12] U.S. Department of Defense, *2022 National Defense Strategy of the United States of America* (October 27, 2022), https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf.
[13] U.S. Department of Defense, *2022 National Defense Strategy*.
[14] Tong Zhao, "Untangling the Nuclear Knot: A Constructive Agenda for Managing China's Nuclear Relations with the United States and Its Allies," Carnegie Endowment for International Peace, September 23, 2026, https://carnegieendowment.org/research/2026/09/untangling-the-nuclear-knot-a-constructive-agenda-for-managing-chinas-nuclear-relations-with-the-united-states-and-its-allies#footnote-6.
[15] U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025*, (December 23, 2025), https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF; Congressional Commission on the Strategic Posture of the United States, *America's Strategic Posture – The Final Report of the Congressional Commission on the Strategic Posture of the United States* (October 2023), https://www.ida.org/assets/2026/06/18084611/Strategic-Posture-Commission-Report.pdf#page=21.
[16] State Council Information Office of the People's Republic of China, *China's Arms Control, Disarmament, and Nonproliferation in the New Era*, (November 2025), http://english.scio.gov.cn/whitepapers/2025-11/27/content_118198082.html.
[17] Zhao, 'Untangling the Nuclear Knot."

or that approximates the strategic effects of a nuclear strike."[18] In addition, although Chinese official documents do not explicitly address the cyber vulnerability of nuclear forces in detail, Chinese military analysts have highlighted how the increasing informatisation of the armed forces may lead to additional vulnerability to adversary cyberattacks.[19] Mirroring the position of the United States, China regards the US as its primary cyber threat.[20] The limited reports published through organisations such as the Cyber Security Association of China and the China Cybersecurity Industry Alliance, have so far predominantly focused on naming and shaming alleged cyberattacks originating from the United States.[21]

ESCALATION PATHWAYS

While not explicitly described in official doctrines, at the expert level, there are already established discussions examining how cyber operations could interact with nuclear escalation. Several potential pathways have been identified.

These include cyber espionage targeting NC3 systems and their connected networks for intelligence collection; cyber operations against dual-use systems, even when the operation is not intended to interfere with nuclear operations; and cyber operations conducted by third parties seeking to manipulate or provoke a conflict between nuclear-armed states.[22] Cyber threats can also be differentiated according to their intended effects. Some operations may seek to disable nuclear systems or prevent them from functioning as intended, a scenario generally associated with state actors, while others could seek to manipulate nuclear systems in ways that could contribute to an unintended

[18] U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (October 19, 2023), https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

[19] Henrik Ståhane Hiim et al., "The Dynamics of an Entangled Security Dilemma: China's Changing Nuclear Posture," *International Security* 47, no.4 (Spring 2023), https://doi.org/10.1162/isec_a_00457.

[20] Ministry of Foreign Affairs of the People's Republic of China, "2025 年 8 月 1 日外交部发言人郭嘉昆主持例行记者会 [Foreign Ministry Spokesperson Guo Jia-kun hosted a regular press conference on August 1, 2025]," August 1, 2025, https://www.mfa.gov.cn/web/wjdt_674879/fyrbt_674889/202508/t20250801_11681249.shtml.

[21] "美情报机构频繁对我国防军工领域实施网络攻击窃密 [US intelligence agencies frequently conduct cyberattacks to steal secrets from China's defense and military industry]," Xinhua, August 1, 2025, https://www.news.cn/20250801/dee28ed16fc84d10981dcd9d0a722f6c/c.html; China Cybersecurity Industry Alliance, *Review of Cyberattacks from US Intelligence Agencies – Based on Global Cybersecurity Communities' Analyses'* (April 2023), http://www.china-cia.org.cn/AQLMWebManage/Resources/kindeditor/attached/file/20230411/20230411080719_9921.pdf; China Cybersecurity Industry Alliance, *Mobile Cyberattacks Conducted by US Intelligence Agencies* (March 2025), https://www.news.cn/world/20250325/02ba448744ac4b75a81df613a88b4d26/2025032522b55fd15b244a5fac54e424c62be9b7_1616350dfed1c44ba786a82d574c86c30f.pdf.

[22] Fei Su et al., *Pragmatic Approaches to Governance at the Artificial Intelligence–Nuclear Nexus* (SIPRI, October 2025), https://doi.org/10.55163/BCHM4674.

launch or detonation.[23] Moreover, there are also concerns as to whether the potential vulnerability of nuclear weapons systems to cyberattacks, and the difficulty of detecting those attacks, creates uncertainty about the survivability and reliability of a state's second-strike capability.[24] Such uncertainty could, in turn, create incentives for precautionary or first use, particularly during periods of heightened crisis.

Apart from this, the development of technology is also introducing additional layers of complexity. AI-enabled cyber capabilities, for example, could increase the speed, scale, and sophistication of cyber operations, including the identification and exploitation of zero-day vulnerabilities.[25] In a recent report, Anthropic described what it characterised as the first known "Agentic-AI cyberattack", allegedly conducted by a Chinese state-sponsored hacking group identified as GTG-1002. According to Anthropic, the operation involved a high degree of autonomy, with limited human involvement remaining primarily in decisions such as target selection and approval of data exfiltration.[26] Such developments also raise concerns about unintended escalation. An AI-enabled cyber operation intended for prepositioning, a tactic to infiltrate adversary's system with the potential for future destructive operation, could lead to unintended implications due to technical loss of control, or the launch of an attack without authorisation.[27]

CYBER INCIDENTS – VIASAT AND BEIJING TIME

While acknowledging that many cyber incidents remain unreported or classified, known cases indicate a growing trend of deliberate attacks against satellite infrastructure which is dual-use in nature, and is critical to conventional and/or nuclear forces.[28] This trend has been reinforced by the war in Ukraine, where cyberattacks against satellite networks have been used to facilitate kinetic military operations.[29] Although such attacks can be highly escalatory, the case of the Salt Typhoon attack against the United States' Viasat

[23] Andrew Futter, *Managing the Cyber-Nuclear Nexus*, European Leadership Network, July 24, 2019, https://europeanleadershipnetwork.org/wp-content/uploads/2019/07/26072019-Managing-the-Cyber-Nuclear-Nexus.pdf.
[24] Jame Johnson and Eleanor Krabill, "AI, Cyberspace, and Nuclear Weapons," War on the Rocks, January 31, 2020, https://warontherocks.com/ai-cyberspace-and-nuclear-weapons/.
[25] Mikel Rodriguez et al., "A Framework for Evaluating Emerging Cyberattack Capabilities of AI," preprint, arXiv:2503.11917v3, April 21, 2025, https://arxiv.org/html/2503.11917v3.
[26] "Disrupting the first reported AI-orchestrated cyber espionage campaign," Anthropic, November 13, 2025, https://www.anthropic.com/news/disrupting-AI-espionage.
[27] Sven Herpig, *Assessing Irresponsibility in Cyber Operations* (Interface, December 1, 2025), https://www.interface-eu.org/publications/cyber-red-flags; Melanie W. Sisson and Tianjiao Jiang, "Advancing human control of military AI," Brookings, Sepember 9, 2026, https://www.brookings.edu/articles/advancing-human-control-of-military-ai/.
[28] Saalman et al., *Mapping Cyber-related Missile and Satellite Incidents.*
[29] Ariel (Eli) Levite, "Integrating Cyber into Warfighting: Some Early Takeaways from the Ukraine Conflict," Carnegie Endowment for International Peace, April 18, 2023, https://carnegieendowment.org/research/2023/04/integrating-cyber-into-warfighting-some-early-takeaways-from-the-ukraine-conflict.

Satellite network shows how escalation can be restrained during peacetime through public attribution and sanctions. The second case of the "Beijing Time" incident further illustrates that attacks on civilian infrastructure can also have strategic implications.

Salt Typhoon Viasat Incident

In early 2025, Viasat – a major satellite service provider for both civilian and military communications, discovered that an unknown actor had gained unauthorised access to its network. Identified in June 2025, this attack was reportedly conducted by Salt Typhoon, which is widely attributed as being a Chinese state-sponsored cyber group with a link to China's Ministry of State Security (MSS).[30] The intrusion reportedly exploited remote-management links used to operate satellite systems, with access to satellite telemetry and control data which could have been monitored or manipulated.[31] However, Viasat found no evidence that their customers were affected or that an outage occurred.[32] The intrusion has been assessed as primarily oriented towards intelligence gathering rather than immediate sabotage. The US response to the broader Salt Typhoon campaign, including public attribution and targeted sanctions, also illustrates the potential for calibrated escalation management.[33] However, concerns remain that the operation may have served to test the resilience of networks on which the United States military could rely as backups during a crisis.[34]

Beijing Time

In October 2025, China's MSS revealed a cyber operation targeting the National Time Service Center (NTSC), which generates and maintains Beijing Time.[35] According to

---

[30] "NSA and Others Provide Guidance to Counter China State-Sponsored Actors Targeting Critical Infrastructure Organizations," US National Security Agency, August 27, 2025, https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/article/4287371/nsa-and-others-provide-guidance-to-counter-china-state-sponsored-actors-targeti/; New Jersey Cybersecurity and Communications Integration Cell, *Salt Typhoon APT: A Strategic Threat Assessment* (October 2025), https://www.cyber.nj.gov/home/showpublisheddocument/1165/638955341897900000; Jamie Tarabay, "Viasat Identified as Victim in Sweeping Phone Hack Tied to China," Bloomberg, June 17, 2025, https://www.bloomberg.com/news/articles/2025-06-17/viasat-identified-as-victim-in-china-linked-salt-typhoon-hack.

[31] "Salt Typhoon Reached Viasat Through the Ground Segment," CYSAT, September 16, 2026, https://cysat.eu/news/salt-typhoon-viasat-ground-segment.

[32] "Viasat identified as victim in Chinese Salt Typhoon cyberespionage, Bloomberg News reports," Reuters, June 18, 2025, https://www.reuters.com/business/media-telecom/viasat-identified-victim-chinese-salt-typhoon-cyberespionage-bloomberg-news-2025-06-17/.

[33] U.S. Department of the Treasury, "Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise," January 17, 2025, https://home.treasury.gov/news/press-releases/jy2792.

[34] New Jersey Cybersecurity and Communications Integration Cell, *Salt Typhoon APT*.

[35] Ravie Lakshmanan, "MSS Claims NSA Used 42 Cyber Tools in Multi-Stage Attack on Beijing Time Systems," *The Hacker News*, October 20, 2025, https://thehackernews.com/2025/10/mss-claims-nsa-used-42-cyber-tools-in.html.

MSS, the operation began in March 2022 and targeted both the NTSC networks and internal networks and the High-Precision Ground-Based Timing System. The operation reportedly escalated, with Chinese authorities claiming that the attackers deployed a new cyber-operations platform using 42 specialised tools designed for persistence, lateral movement, and covert communications.[36] Chinese officials highlighted that a successful compromise of NTSC could have cascading effects on communications, financial systems, power, transportation, and space launch failures, given the dependence of these systems on precision timing.[37] Disruption could also affect the performance of Beidou Navigation Satellite system, which supports civilian and military operations including People's Liberation Army's operations, such as precision strikes, operations in distant theatres and C2 and communications.[38] This case is notable as one of the few cases in which China has publicly attributed a cyber operation to a foreign state. While the public attribution may serve broader political purposes, it also provides an indication of the types of cyber operations and critical infrastructure that China considers potentially escalatory.

CONCLUSION

It seems that neither the United States nor Chinese nuclear doctrines, nor the recent cyber incidents examined, provide a clear threshold for when cyber operations against strategically relevant infrastructure become unacceptable or contribute to escalation. There appears to remain some political room for containing such incidents within the cyber domain rather than allowing them to spill over into broader military confrontation. However, this should not be taken for granted. As cyber capabilities become more sophisticated and nuclear and conventional military systems become increasingly digitalised and automated, the potential consequences, such as spillover effects, of cyber operations may become more difficult to contain.

This creates a need for greater clarity regarding escalatory thresholds. States would benefit from a more accurate understanding of which types of cyber operations (particularly those affecting dual-use infrastructures) are considered unacceptable. While Russian officials have claimed that "Quasi-civilian infrastructure may become a

[36] Cui Jia, "Ministry exposes US plot to tamper with Beijing Time," China Daily, October 19, 2025, https://www.chinadailyhk.com/hk/article/621968.
[37] "China's state security authorities uncover case of major cyberattack from US NSA employing state-level cyber-espionage weapons targeting 'Beijing Time': MSS," Global Times, October 19, 2025, https://www.globaltimes.cn/page/202510/1345993.shtml.
[38] "Chinese naval fleets entered the South China Sea and played a role in the BeiDou system [中国海军舰艇编队进入南海 北斗系统发挥作用]," Qingdao News, February 2, 2013, https://www.qingdaonews.com/content/2013-02/02/content_9597354.htm; Kevin Pollpeter, *To Be More Precise: BEIDOU, GPS, and the Emerging Competition in Satellite-Based PNT*, China Aerospace Studies Institute, May 20, 2024, https://www.airuniversity.af.edu/CASI/Display/Article/3778910/to-be-more-precise-beidou-gps-and-the-emerging-competition-in-satellite-based-p/.

legitimate target for retaliation",[39] there is no clear consensus on where such boundaries should be drawn. This raises the question of whether certain dual-use infrastructure, such as satellite services, should be treated as off-limits given their potential to contribute to escalation.

Crisis management mechanisms could also play an important role. Dedicated communication channels could provide states with opportunities to clarify incidents, signal intentions, and prevent misinterpretation during periods of heightened tension. The recent proposal between China and the United States for establishing an AI hotline and notification mechanism to alert each other about high-risk AI incidents threatening national security provides a potential model for extending similar arrangements to cyber incidents involving military or dual-use infrastructure.[40]

[39] Joey Roulette, "Russia's anti-satellite threat tests laws of war in space," Reuters, October 28, 2022, https://www.reuters.com/world/russias-anti-satellite-threat-tests-laws-war-space-2022-10-28/

[40] Lin Feng, "US, China plan AI incident channel as fierce competition tests room for cooperation," VOA, October 5, 2026, https://www.voanews.com/a/us-china-plan-ai-incident-channel-as-fierce-competition-tests-room-for-cooperation/8208082.html.

ABOUT THE AUTHOR

Fei Su is a Senior Researcher at the China and Asia Security Programme of Stockholm International Peace Research Institute. She joined SIPRI as a Research Assistant in March 2015 and was based in Beijing. Prior to joining SIPRI, she lived and studied in Seoul for three years, where she strengthened her fluency in Korean. She holds a MA in Public Administration from Graduate School of Public Administration at Seoul National University, focusing on governance. She wrote her Korean-language dissertation on the impact of government size on corruption in China.

Fei's current research interests focus on regional security issues in East Asia with a special interest in North Korea, China's foreign and security policy, maritime security, cybersecurity and AI-nuclear nexus. She is currently a member of the Transatlantic Cyber Forum (TCF) working group on "Irresponsible Behavior During Cyber Operations" at Interface and has been admitted to the 2025-2026 cohort of the Arms Control Negotiation Academy (ACONA) Fellowship.

ABOUT APLN

The **Asia-Pacific Leadership Network (APLN)** is a Seoul-based organisation and network of political, military, diplomatic leaders, and experts from across the Asia-Pacific region, working to address global security challenges, with a particular focus on reducing and eliminating nuclear weapons risks. The mission of APLN is to inform and stimulate debate, influence action, and propose policy recommendations designed to address regional security threats, with an emphasis on nuclear and other WMD (weapon of mass destruction) threats, and to do everything possible to achieve a world in which nuclear weapons and other WMDs are contained, diminished, and eventually eliminated.

