Commentary
December 26, 2024

US-China: On the brink of a major cyber war?

Yauheni Preiherman

Originally published by Caliber.az

Summary

The escalating cyber rivalry between Washington and Beijing is starting to echo the nuclear standoff of the Cold War in its political dimension. Depending on the decisions made by the Trump administration in the coming months, this situation could either lead to a dangerous and rapid escalation or, conversely, pave the way for de-escalation and active diplomacy.

In early December, reports emerged in the U.S. media revealing that at least eight major American telecommunication networks had been targeted by a cyberattack. The attack was described as unprecedented in terms of its scale and depth of infiltration. The news hit like a bombshell. However, with the Christmas holidays approaching and the transfer of power to Donald Trump's new administration imminent, the information bomb seemed more like a delayed fuse. While politicians and commentators have loudly expressed their shock and called for dramatic retaliatory measures, it appears that no concrete decisions have been made in this regard so far.

If such actions are ultimately taken, the world may face a major escalation of cyber tensions in the new year. Predicting the course of events in this scenario is difficult, as there has never been direct "combat" in cyberspace between the world's leading powers.

> As a result, these events could either lead to a catastrophic surge in tensions, escalating to the level of full-scale war or, conversely, act as a trigger for de-escalation of the already highly charged geopolitical climate.

The largest cyberattack in history?

U.S. media reports, citing intelligence agencies, claim that the massive cyberattack was carried out by the Chinese hacker group Salt Typhoon (a name coined by American authorities). According to the released information, the group gained access to the private databases of at least eight major telecommunication companies, including T-Mobile, Verizon, Lumen, and AT&T. It is estimated that metadata—such as information about calls and messages, rather than their actual content—of over 1 million individuals was compromised. Most notably, among those whose phones may have been targeted were numerous high-ranking politicians and officials, including newly elected President Donald Trump and his Vice President, JD Vance.

According to media reports, the scale of the attack is so vast that U.S. Senate Intelligence Committee Chairman Mark Warner called it the "worst telecom hack in our nation's history — by far." Likely future Secretary of State Senator Marco Rubio described it as "the most disturbing and widespread incursion into our telecommunication systems in the history of the world, not just the country." Similar assessments were made by intelligence officials from Australia, Canada, and New Zealand.

Despite this, efforts to fully stop the data breach have not yet succeeded, even though U.S. intelligence agencies are said to have been aware of the incident since September. This is likely due to both the technical complexity of the task and the caution exercised by American IT specialists. The latter are focused on minimizing the risk of further damage to the country's telecommunication infrastructure, while simultaneously gathering as much information as possible on the methods used by the hackers.

Notably, this is not the first time in recent years that Washington has accused Chinese hacker groups of launching cyberattacks on critical U.S. infrastructure. These accusations are typically accompanied by media emphasis on the alleged affiliation of these groups with the Chinese government (similar language is often used in reference to other non-governmental actors, such as those from Russia). For example, in May 2023, Microsoft reported a Chinese cyberattack targeting water and transportation infrastructure across the U.S. Then, in September of this year, the FBI Director accused groups "working at the direction of the Chinese government" of gaining control over hundreds of thousands of internet-connected devices, including video cameras and data storage equipment.

The Chinese side has denied any involvement in the incident. A spokesperson for the Chinese Embassy in Washington dismissed the accusations against his country as "irrational" and emphasized that China itself is routinely targeted by cyberattacks.

> However, in the U.S., at least in the public domain, there is little dissent: everyone is convinced that the infiltration of telecommunication companies' information systems was carried out by Salt Typhoon, with the aim of gathering sensitive intelligence on behalf of the Chinese government.

Against this backdrop, there have been bellicose calls directed at both the current Biden administration and the incoming Trump administration to respond in a way that leaves a lasting impact. For example, Republican Mark Green, Chairman of the House Committee on Homeland Security, has urged the executive branch to launch an offensive against China in cyberspace, rather than limiting itself to defensive actions aimed solely at protecting U.S. infrastructure. According to him, Washington must demonstrate to the world that it has the means to retaliate and "put a knife to China's throat." Many other politicians, journalists, and experts have echoed similar sentiments.

Whether the White House will heed these calls remains to be seen in the near future. The U.S. will be under Democratic administration for another month, so it's possible that it may take some proactive actions during this time. Traditionally, outgoing administrations refrain from making decisions with long-term consequences in the final months of their term. However, this does not seem to apply to the Biden administration. As seen in the examples of crises in the Middle East and the war in Ukraine, it has instead shown increased activity in its final weeks, likely aiming for some public relations successes while simultaneously limiting the future manoeuvrability of the incoming Trump administration.

At the moment, however, the current administration has refrained from extensive comments or concrete decisions regarding the hacker group Salt Typhoon and the entire situation tied to it. Therefore, it is likely that the file will simply be handed over to the incoming administration. The Republican government, in any case, will need to pay increased attention to cybersecurity as a whole, and to countering China in this area.

Firstly, given the deep integration of online technologies into various aspects of life, the issue of cyberspace has become increasingly significant for the national security of any state. This is especially true for the U.S., as well as China, both of which are vying for leadership positions globally, including in information technology. *Secondly*, the growing public and political resonance surrounding the Salt Typhoon case, as well as previous instances of cyberattacks in which American media blamed Beijing, will likely pressure the Trump administration to take decisive action.

> Therefore, the likelihood of sharp and large-scale retaliatory measures from Washington in the coming months is indeed high. This, in turn, carries the risk of serious escalation.

Such escalation could quickly evolve into an unprecedented cyberwar between the world's largest powers. In certain hypothetical scenarios, this confrontation could even spill over from the online realm and provoke kinetic clashes in the real world.

Cyberspace as the new nuclear weapon

While such catastrophic scenarios may seem unlikely at present, they remain no less dangerous. This is a reality that must be acknowledged by anyone advocating for "offensive action, not just defence."

Even from the quote above by Republican Congressman Mark Green, it's clear that the growing cyber confrontation is widely perceived through the same lens as traditional military conflict. The logic of the opposing sides is the same. In particular, the same deterrence strategy is at play: the goal is to demonstrate our superior capabilities and unwavering will to deploy them in defence of our interests. Opponents, in turn, always adopt the same reasoning.

As in the purely military realm, the focus of opposing countries on mutual forceful deterrence leads to the escalation of what is known as the security dilemma (or security spiral). In other words, each side increases its own military capabilities and constantly demonstrates its readiness to fully deploy them solely for the protection and assurance of its security. However, from the perspective of the opposing side, this appears as nothing less than a threatening activity, which may create material and political conditions for aggression. As a result, the second side continues to build up its own forces and resources, constantly seeking vulnerabilities in the enemy's systems.

Such a confrontation quickly evolves into a spiralling process. With each new turn, the level of tension rises, and with it, the likelihood of real conflict. Psychologically, with every cycle, it becomes harder for the participants to see anything in the opposing side other than an implacable enemy bent on complete destruction. And if that is the case—what room is there for negotiations?

Breaking the vicious cycle of spiralling escalation can be achieved either through an extraordinary diplomatic effort from both sides or as a result of a major crisis that brings both adversaries to realize the inevitable, unacceptable losses they would suffer if the

spiral continues. More precisely, it is only the combination of these two factors that can play a stabilizing role: initially, the crisis forces politicians to recognize the imminent catastrophe, after which they grant diplomats the mandate to fully perform their work.

> In the mid-20th century, these factors converged after the U.S. and the USSR developed nuclear arsenals capable of destroying each other and all of human civilization.

With some degree of approximation, one could argue that in the 21st century, cyber weapons could play a similar role. It's clear that a direct comparison of the destructive potential of these technologies seems inappropriate. However, from a political standpoint, they are still comparable.

Just like nuclear weapons in the mid-20th century, cyberspace today is technologically advanced but politically poorly understood. Much like the nuclear realm at that time, there is still no comprehensive framework of international agreements to sufficiently regulate interaction and competition in cyberspace. At the same time, the vulnerability of both states and individuals, should the situation in cyberspace spiral out of control, is evidently very high.

Therefore, while the world may face the looming risk of a large-scale cyberwar in the coming months, the current situation also presents an opportunity to lay the groundwork for a constructive negotiation process. This would involve de-escalating tensions and establishing professional and political channels to foster mutual trust, not only between Washington and Beijing but also in a multilateral context, which is especially important given the emerging multipolarity. Ultimately, the direction in which the pendulum of future events swings will largely depend on the decisions made by the incoming U.S. administration under Donald Trump.

Yauheni Preiherman
Director, Minsk Dialogue Council on International Relations