Chapter 3, Problem II: Malicious Cyber Conduct

Cyberattacks on U.S. targets appear to have increased since President Biden took office. For example, in March 2021, Chinese hackers breached Microsoft's email software, used by thousands of companies, governments, and military contractors. In May, Russian hackers attacked the Colonial Pipeline Company, leading to fuel shortages across the U.S. east coast. The Biden Administration has responded to this uptick in malicious cyber conduct by making cybersecurity a top priority. In May 2021, it issued an executive order that reduces barriers to sharing threat information and mandates better commercial security standards. It has also issued a number of public documents that explain how to reduce cyber vulnerabilities. One such document consists of highly detailed information about Chinese tactics for infiltrating private networks.

In June 2021, President Biden spoke directly to Russian President Vladimir Putin to demand that Russia clamp down on criminal hackers operating in its territory. Although Russia's response is difficult to assess, there is evidence that it has taken steps to address the problem.

The dynamic with China has been different. On July 19, the U.S. government "[a]ttribut[ed] with a high degree of confidence that malicious cyber actors affiliated with PRC's [Ministry of State Security] conducted cyber espionage operations utilizing the zero-day vulnerabilities in Microsoft Exchange Server disclosed in early March 2021." It coordinated that announcement with a coalition of other countries. On the very same day, Canada, United Kingdom, Australia, Japan, and New Zealand each issued similar statements attributing the Microsoft attack to the Chinese Government.

The European Union also issued a statement about the Microsoft attack on July 19. However, it did not attribute the attack to China. It asserted that "malicious cyber activities that significantly affected our economy, security, democracy and society at large . . . have been undertaken from the territory of China." In addition, the EU "urge[d] the Chinese authorities to adhere to ["the norms of responsible state behaviour as endorsed by all UN member states"] and not allow its territory to be used for malicious cyber activities, and take all appropriate measures and reasonably available and feasible steps to detect, investigate and address the situation."

In addition, the North Atlantic Treaty Organization (NATO) issued a statement on July 19. The NATO statement reads:

> 1. We observe with increasing concern that cyber threats to the security of the Alliance are complex, destructive, coercive, and becoming ever more frequent. This has been recently illustrated by ransomware incidents and other malicious cyber activity, targeting our critical infrastructure and democratic institutions, as well as exploiting weaknesses in hardware and software supply chains.
>
> 2. We condemn such malicious cyber activities which are designed to destabilize and harm Euro-Atlantic security and disrupt the daily lives of our citizens. We

> use NATO as a platform for political consultations, to share concerns about malicious cyber activities, to exchange national approaches and responses, as well as to consider possible collective responses. Reaffirming NATO's defensive mandate, the Alliance is determined to employ the full range of capabilities, as applicable, at all times to actively deter, defend against, and counter the full spectrum of cyber threats, in accordance with international law. NATO will continue to adapt to the evolving cyber threat landscape, which is affected by both state and non-state actors, including state-sponsored. We remain committed to uphold strong national cyber defences, including through full implementation of NATO's Cyber Defence Pledge.
>
> 3. We stand in solidarity with all those who have been affected by recent malicious cyber activities including the Microsoft Exchange Server compromise. Such malicious cyber activities undermine security, confidence and stability in cyberspace. We acknowledge national statements by Allies, such as Canada, the United Kingdom, and the United States, attributing responsibility for the Microsoft Exchange Server compromise to the People's Republic of China. In line with our recent Brussels Summit Communiqué, we call on all States, including China, to uphold their international commitments and obligations and to act responsibly in the international system, including in cyberspace. We also reiterate our willingness to maintain a constructive dialogue with China based on our interests, on areas of relevance to the Alliance such as cyber threats, and on common challenges.
>
> 4. We promote a free, open, peaceful and secure cyberspace, and pursue efforts to enhance stability and reduce the risk of conflict by promoting respect for international law and the voluntary norms of responsible state behaviour in cyberspace, as recognized by all member states of the United Nations. We are working together as an Alliance and with like-minded partners to address these challenges. All States have an important role to play in promoting and upholding these voluntary norms of responsible state behaviour.

China responded to the claims against it by asserting that they were "groundless," "fabricated" a "malicious smear against China on cybersecurity." A Chinese government spokesperson added that "it is irresponsible and ill-intentioned to accuse a particular party when there is no sufficient evidence around."

Notes and Questions

1. One noteworthy feature of the claims against China is that they do not expressly accuse China of violating international law. Why might countries attribute cyber conduct to China—and why might China deny any role in it—without specific mention of international law? How, if at all, would the dynamic be different if the complaining states expressly declared China's conduct to be unlawful?

2. The governments and organizations that spent the time, energy, and political capital on these statements presumably think they serve a useful function. What function might they serve?