The US-Japan Virtual Forum on Cybersecurity Cooperation:
Beyond the Tokyo Olympics
Virtual Workshop | Aug. 17-19, 2021 (US) / Aug. 18-20, 2021 (Japan)

Key Findings

On Aug. 17-19, 2021, Pacific Forum hosted a three-day virtual workshop joined by over 70 individuals representing government, industry, academia, and civil society from the Indo-Pacific. The first two days were closed-door, while the final day's proceedings were open to the public. The virtual dialogue featured renowned Japanese and American speakers, who tackled key dimensions of cybersecurity cooperation under the US-Japan alliance. To test and operationalize the concepts and deliberations and formulate actionable and pragmatic policy insights, a cybersecurity tabletop exercise was also conducted as part of the workshop.

Key Findings from the workshop can be found below:

The State of Cybersecurity Cooperation

The Tokyo 2020-2021 Olympics will be remembered in the modern history of international sporting events as an event like no other. Against the backdrop of a global pandemic, strategic reordering, socio-technological disruptions, and Japan's own brewing domestic opposition to the games, the global sports spectacle took place and redefined resilience in the new normal. Speaking of resilience, cybersecurity was a cornerstone of Japan's hosting and a top priority for ensuring the smooth execution of the games—a resolve that will shape its cyber policy outlook in decades ahead.

After the Summer Games Japan appears determined to maintain its momentum toward achieving cyber resiliency. Currently, Japan's 2021 cyber security strategy is open for public consultation. Through a cursory glance at the 2021 draft, a few major observations come to the fore. First is an increase in the sense of urgency to address Chinese, Russian, and North Korean cyber activities. The propensity of the Japanese government to name and shame specific state actors signals its intent to avoid ambiguity, which is a dramatic shift in its cyber policy. However, the draft remains consistent with the 2018 cyber strategy, with a few developments on data policy. The current draft still does not outline any plans to develop or enhance Japan's offensive cyber capabilities but emphasizes continuing, if not elevated efforts on improving cyber-deterrence. To this end, the US-Japan alliance remains a key plank in Japan's overall cyber policy. The 2021 draft has shown increased government-to-government cooperation on national data security policy, and as such the Japanese Ministry of Defense and the US Department of Defense maybe even closer to establishing a more credible data-sharing cooperative framework. As expected, there remain strong expectations for multilateral cooperation with the United Nations, and partner countries, like India and Australia, to create a stronger cyber defense to identify and possibly hold attackers accountable.

The dramatic evolution of the cyber threat landscape over the course of the pandemic--which expanded the conventional classification of critical national infrastructure--combined with the rising influence of non-state actors makes dissecting the many facets of cybersecurity even more necessary, especially under the matrix of US-Japan cooperation.

When deliberating Japanese-US cooperation and critical infrastructure, several considerations emerge. Foremost, what should the channels of coordination between the US and Japan in cybersecurity look like? This question considers the seniority of ministers who should deliberate on cybersecurity matters and the frequency of meetings. Some experts have expressed their preference for more technical, regular meetings. They have also discussed the benefits of greater standards settings and how both allies continue to exchange views in maintaining stability in the cyber domain. The unprecedented impact of COVID-19 has also bred new cybersecurity challenges, especially vulnerabilities related to telework. The pandemic has resulted in individuals spending much more time online, providing malicious actors with greater attack surfaces. Amid the rapid expansion of remote working arrangements, many employees still lack cyber hygiene, and, in some instances, this has led to corporate data being mistakenly uploaded to non-work applications. The emergence of new, more virulent, strains of the coronavirus is also a critical consideration for US-Japan cooperation. Hacking operations against pharmaceutical and scientific organizations to steal proprietary information related to vaccine research and development are of utmost concern. Additionally, the proliferation, efficacy, and dangers of ransomware—especially if it contaminates critical infrastructure—are all pressing concerns for the US and Japan.

Ransomware attacks are a particularly pernicious, and growing, cyber threat, with 58% of American and 52% of Japanese companies reporting such incidents between 2020 - 2021. Among those reported, only 24% of ransomware attacks could be stopped before encryption, meaning that three-quarters of attacks were successful. Across industries, manufacturing, health care, and education have the lowest cybersecurity maturity. In healthcare, 86% of health care institutions do not use any email scanning filtering tool, leaving the sector vulnerable to espionage and ransomware. In fact, 48% of US hospitals have had to disconnect their networks in the past six months because of ransomware attacks.

Cybersecurity professionals have also observed a steady growth of supply chain attacks and the emergence of ransomware as a service. Supply chain attacks saw an increase in popularity among state actors, and often target trusted vendors that provide systems and software for target institutions. The growth of ransomware as a service also represents a unique evolution of the technology; it has changed into a form of malicious software that involves gangs of ransomware developers as service providers. As a result, ransomware has become accessible on a massive scale because people using it no longer need to develop it themselves. To deal with this, policymakers need to reshape online conditions to hinder malicious actors and re-engage in the initiative. Here, the importance of US-Japan coordination to start advocating for international norms in relation to ransomware attacks would be paramount.

Submarine cables are an essential conduit connecting cyberspace telecommunication signals with physical land-based stations. Approximately 99% of international traffic, including considerable military communications, passes through undersea cables. Three companies—Subcom, NEC, and Alcatel Submarine Networks, from the US, Japan, and the EU, respectively—

control 95% of the cables, however, new Chinese companies are gaining ground. There are several threats to undersea cables. Physically cutting cables is not uncommon; it happens accidentally almost every day, however, malicious actors may also intentionally cut them. This might happen in emergency situations when an adversary is looking to disrupt communications. Government and non-state actors have also been known to tap cables, but optic communications are extremely sensitive and difficult to capture. Current concerns stem from possibly compromised cables, Submarine Line Terminal Equipment (SLTE), and data transmissions that pass through. Data capture can be made easier by establishing a connection to SLTEs in a data capturing center. The US remains concerned about China playing out this scenario in Hong Kong.

Data centers, as the connective tissue for data, are another concern for state actors. Over 20,000 nation state-attributable cyber-attacks have been carried out, with Russia, China, Iran, and North Korea considered the "big four" actors in this domain. These attacks are by nature intelligence operations and rarely target critical infrastructure. In the past year, Indo-Pacific countries have been targeted in about 244 attacks. For Japan, North Korea is the most active perpetrator of these attacks (61%), followed by Russia and China. These attacks usually target government agencies, think tanks, defense institutions, and academics. Interestingly, a higher than average (25%) figure of cyberattacks aimed at Japan has targeted critical infrastructures.

Cybersecurity Tabletop Exercise

The second day of the US-Japan Cyber Security Conference featured a table-top exercise (TTX) where participants were presented with a scenario and then broken into three teams: Team Japan, Team USA, and Team IOC. Under time constraints and with limited information, each team was given a set of questions and tasked to formulate the best possible cyber policy recommendations.

In the given scenario, the Japanese Olympic Committee (JOC), as the host nation for the 2020-21 Tokyo Olympics, suffered a major cyberattack. The cyberattack targeted the Games organizers, advisors, logistics services, and sponsors, as well as delivering malware to the executive board members of the JOC. With the cyberattack threatening to overshadow the Closing Ceremony of the Games. Japan is confronted with the difficult choice of protecting its international reputation while navigating the evolving cyber threat landscape and balancing its own interests in lock-step with the US.

Team Japan and Team USA responded to the following questions:

1. Identify up to three remediation strategies that your team should undertake within the 24-36 hours following the incident.
2. Identify up to three actions that your team wants the other teams TO TAKE.
3. Identify up to three actions that your team wants the other teams NOT TO TAKE.
4. With a heightened sense of urgency, identify up to three policy recommendations that your team should pursue in close coordination with the other teams—taking into full consideration inherent characteristics such as comparative advantages and political limitations—to address the cyberattack.

Team IOC was presented with the following set of questions:

1. Identify up to three remediation strategies that your team should undertake within the 24-36 hours following the incident.
2. Identify up to three actions that your team wants Japan TO TAKE.

3. Identify up to three actions that your team wants Japan NOT TO TAKE.
4. With a heightened sense of urgency, identify up to three policy recommendations that Team IOC should pursue in close coordination with JAPAN--taking into full consideration the need to successfully close the Olympics and other political and economic limitations--in the aftermath of the cyberattack.

Team the USA

Team USA identified attribution, immediate coordination, and ensuring that the attacks have been halted as the three most urgent steps. That being said, the team recognized that before proper attribution could take place due diligence must be conducted. Team USA also acknowledged the weaknesses of Japanese cyber security in the past, with concerns over how such failures could impact cooperation. Team USA wanted to ensure Japan was arresting the cyber-attacks and that critical information had been secured.

The team sought collaboration between the US and Japan in gathering forensic information on the hack itself. The group also noted that the IOC lacks the ability to retaliate against a cyberattack and would also not consider such a response to be desirable. Team USA also wanted none of the other teams to publicize the attack, but also expressed concern over Japan's historical reticence to engage in attribution until Washington had first taken concrete steps in the process. Finally, in coordination with the other teams, Team USA sought to ensure such attacks would not take place again, implement an after-action response review to see how they could have responded better, and develop an offensive response for future hacking incidents.

Team IOC

In the 24-36 hours following the incident, Team IOC deemed it critical to undertake a baseline risk assessment to establish any ongoing risks to athletes and officials with the sole intent of preventing further harm. The team also wanted to clarify whose Computer Emergency Response Teams would be tasked with the response to detected cyber-attacks and develop backchannels with national computer emergency response teams (CERTs) to allow for notifications on potential cyberattacks during or even between games. The team also found it important to share relevant information from the attack between the Olympic Committee and Japanese officials and establish a monitoring process to implement a pre-agreed incident response program. Team IOC wanted Japan to consult with international organizations like Interpol to investigate the incident. It also implored Team Japan to sanction any responsible parties under Section 56 of the Olympic Charter and lodge a case before the International Court of Justice. The team also asked Japan to avoid publicly attributing the attacks to a state actor until the end of the Olympics. This request was designed to help ensure that the reputation of the IOC endures and assist in the smooth execution of the closing ceremony. Team IOC also wanted Team Japan to avoid hacking back, as this would be in contravention of international law and could make the situation worse. Lastly, Team IOC hoped to work in close coordination with Team USA/Japan to ensure the IOC remained informed as the situation unfolds.

Team Japan

Team Japan sought to arrange immediate coordination between the US and the IOC in the 24-36 hours following the attack. Such coordination will be premised on answering essential questions relating to particular channels of cooperation. It would also make certain that the attack was stopped and begin collecting forensic evidence. Given Japan's recent condemnation of Chinese affiliated hacking group APT40, the team saw no reason not to follow the same precedent and attribute the group responsible for the cyberattack on the condition that the threat actor was identified and verified with near-perfect certainty.

Team Japan implored the IOC to share all relevant indicators of compromise. Such items could include IP addresses and email addresses affiliated with the attack. This information would be essential to share with the Japanese Olympic Committee, other Olympics sponsor companies, and defense contractors. Team Japan also planned to reach out to the National Cyber Security Centre, United Kingdom, to ask for any additional information they might have on Russian cyberattacks.

More importantly, Team Japan will consult with the US cybersecurity experts, particularly the defense aerospace communities, to see whether they have any additional information on the attack that could be shared with Japanese defense contractors. Team Japan recommends that a public-private partnership (PPP) help streamline information sharing in instances where private companies are hesitant to share details of their cyber vulnerabilities. The team also recommends developing a joint monitoring center in Honolulu where Japanese private sector defense staff and their US counterparts can sit next to one another and monitor cyber-attacks. Further, Team Japan recommended inviting relevant components of the Japanese private sector to cyber security exercises between the US and Japan. No such structure currently exists, and this could help bolster national security.

In the end, teams had identified their respective course of action, they were presented with an additional set of facts.

After a comprehensive technical investigation and close consultation with the Five Eyes community, the US has decided to name and shame China as the perpetrator of the cyberattack against the JOC that reached the MHI-Lockheed Martin joint-development program. According to a Five Eyes report, the Chinese-linked group, APT12—which has strong ties to the Ministry of State Security—is the primary suspect.

Team Japan, Team US, and Team IOC were asked the following questions:

Does this new information provided change your answers from the first move? If you have changed your answers, please be prepared to explain why in the group presentation.

1. Identify up to three remediation strategies that your team should undertake within the 24-36 hours following the incident.
2. Identify up to three actions that your team wants the other team(s) TO TAKE.
3. Identify up to three actions that your team wants the other team(s) NOT TO TAKE.

4. Identify up to three policy recommendations that your team should pursue in close coordination with the other team(s)—taking into full consideration the latest development—to address the cyberattack.

Team USA's desire for speedy attribution and a delay in the publicizing of the attacks were dropped after the team reconvened. They identified Japanese capitulation to Beijing and the balancing act between attribution and de-escalation as potential areas of concern. The team sought to accommodate Japanese concerns by designating a five-day grace period during which time Team Japan could prepare its own policies and strategies before the public attribution to China would take place. Finally, the team examined the taxonomy of the word "attack" and what the actual implications of its use might mean. The debate between the team primarily centered on the scope and depth of the word "attack" and how its use might affect response formulation.

Team Japan's response to the second set of facts changed little from their initial response. This was especially the case given Japan's new cyber priorities and the central role that naming and attribution plays in this. The group reemphasized the importance of information sharing among allies and organizations, such as the IOC.

Given the IOC's interest in maintaining its apolitical nature, its response between moves did not change significantly. Upon learning that the attack was likely carried out by China, the team proposed the establishment of a specialist tribunal, similar to the World Anti-Doping Agency that would investigate ongoing and future cyber-related attacks as such incidents have become a growing source of concern in the Olympics over the last decade. The creation of such a body could help the IOC remain apolitical while determining what measures it should take in response to the attack and its possible occurrence in the future.

Moving Forward

The current issue in the US-Japan alliance in cybersecurity rests on the inherent risks associated with technological disruptions and innovation brought by the Fourth Industrial Revolution. Add to this, the increasing and pervasive yet stealthy use of offensive capabilities of malicious actors such as China, Russia, and North Korea against the backdrop of a global health crisis. Furthermore, the balkanization of the internet also represents a clear and present danger underpinned by the growing trend of geopolitical tensions being superimposed onto cyberspace.

Strategic latency continues to be a driver of competition as well. Technological changes are a catalyst for increased competition, forcing nation-states to adapt or perish within the realm of cyber. Emerging technologies such as artificial intelligence (AI) present both significant opportunities and challenges as a force multiplier of both offensive and defensive capabilities.

Japan is on the frontlines of the geostrategic tech war between the US and China yet appears unprepared for such a reality. A study published by the International Institute for Strategic Studies' *Cyber Capabilities and National Power: A Net Assessment,* designated Japan in the third tier, ranking its capacity equal to nations such as Indonesia, India, Malaysia, and Vietnam.

While Japan has a strong digital economy, its defense cyber capabilities are inadequate and its offensive capabilities nonexistent due to limitations imposed by its pacifist constitution. Moreover, its myopic definition of cyber-attack continues to hamstring its development in these areas. However, Japan continues to be active in cyber diplomacy. It actively participates in several dialogues with the EU and Australia while engaging with global institutions in the creation of cyber norms. Its provision of foreign aid utilized for technical and policy-centered capacity-building activities and confidence-building measures in Southeast Asia has contributed to maintaining cyber stability in the region.

While there is cooperation on many levels, the US-Japan partnership should continue to strengthen its atmosphere of mutual trust to improve cross-communication and coordination. This goes hand in hand with upgrading intelligence sharing mechanisms as the US adopts more offensive posturing in cyberspace with its Persistent Engagement Cyber Strategy. The alliance's lack of clear plans to handle and respond to critical infrastructure attacks is an area in dire need of closer cooperation. To address this, the US and Japan must review their list of what they consider as critical national infrastructure. The segment of the private sector responsible for managing critical national infrastructure should also be encouraged to become even more proactive and open to information-sharing arrangements. Public-private cybersecurity cooperation should not be limited strictly between the US and Japan; other jurisdictions and parties in the EU and ASEAN should be brought in to expand coordination and cooperation.

Along with ongoing efforts to achieve cyber resiliency and exercising prudence in joint public attribution, the US and Japan must sustain the codification of norms and emphasis of international law to mitigate the spiraling security dilemma in the cyber domain. For its part, Japan should seek to increase its defensive cyber capabilities and continue its cyber diplomacy in the Indo-Pacific. This should be reinforced by deepening its cyber threat intelligence sharing with the US but also with increased cooperation with other capable cyber partners like Australia, India, South Korea, and the EU.

The nexus of cybersecurity and AI present both challenges and prospects in the US-Japan alliance. Based on their Joint-High Level Committee on Science and Technology held in 2019, the two nations have designated quantum science and AI as critical future industries. However, there continues to be a wide margin in terms of AI maturity and a dearth of governance in sharing credible data which creates shortcomings in the development, design, testing, and deployment of AI-infused capabilities.

To remedy this, the US-Japan alliance should create a Cyber-AI focus group to bridge capacity failures and streamline risk management approaches to enable AI systems resilient to emerging threats like adversarial AI. The alliance should develop an accreditation system to ensure that third-party, and commercial vendors operate within a clearly delineated standard of quality control and due diligence. In the long term, the US-Japan alliance must focus on strengthening the fundamental technical basis for AI development that is transparent and inclusive to better understand diverging systems espoused by China and Russia. This would ensure that the human component is kept within the AI development loop, minimize ambiguity biases, and inhibit escalation.

Attachment/Appendix:

US-Japan Cybersecurity Cooperation
Cybersecurity Tabletop Exercise Scenario
August 18 (US) | August 19 (Japan)

The Cyber Wild Card at the Tokyo Olympics

Japanese Translation Here

First Move

It is Aug. 3 and the 2020/2021 Olympics are drawing to a close. Despite mounting domestic and international pressure to cancel the Summer Games, Japan persevered and will soon be concluding a historic event: A successful Olympiad despite a global pandemic, rising domestic COVID-19 cases, low vaccination rollouts, and the emergence of the Delta variant.

There were doubts of course, and high among the concerns, although largely unspoken, was a fear that the Games would be hacked, disrupting the events and embarrassing the hosts. To its credit, Japan's cyber defenses were able to ward off adversaries that may have caused a distraction, delay, or worse.

A few days before the closing ceremony, however, the Japanese Olympic Committee (JOC) as the host nation for the 2020-21 Tokyo Olympics suffered a major cyberattack. Japanese experts launched a forensic examination and found that a threat actor sent a spear-phishing email to various JOC Board Committees privy to vital information regarding the Olympics.

The threat actor delivered sophisticated malware carefully crafted to target top-level Japanese representatives and officials from the public and private sectors in key positions at the JOCUsing a Remote Access Trojan (RAT), the threat actor was able to access computer networks and download files and scripts to exfiltrate highly sensitive data from the targets.

As the Japan Computer, Emergency Response Team Coordination Center (JPCERT/CC) and the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) investigated, it was discovered within 24 hours that the threat actor used codes very similar to a cyber reconnaissance operation linked to Russia's military intelligence agency the GRU. And in October 2020, the UK National Cyber Security Centre confirmed that the GRU-led cyber-reconnaissance had targeted the Games organizers, advisors, logistics services, and sponsors. The recent intrusions went further and delivered malware to the executive board members of the JOC.

JPCERT/CC immediately warned the private sector of the potential effects the cyberattack may have on Critical National Infrastructure. The Chief Information Technology Officer (CITO) of Mitsubishi Heavy Industries (MHI) informed Japanese officials that his team had found identical malware within its servers that hosted critical data on its defense development and procurement program. Although MHI was reluctant to disclose additional details, the information it did

provide suggests that the threat actor was able to access highly classified information concerning the US-Japan joint partnership program aimed at developing a new generation fighter jet based on a hybrid design of the F-35 and F-22.

Assembling the available evidence, Japan CERT and the NISC concluded that the threat actor used the spear-phishing emails to target MHI officials serving in the JOC committee of the Tokyo Olympics 2020, and then penetrate MHI's networks and servers and steal critical data from the joint-development program.

As the Closing Ceremony approached, news broke that China's Ministry of Foreign Affairs had reached out to its Japanese counterparts to explore ways to de-escalate tensions concerning Taiwan. Reliable sources in Japan's Ministry of Foreign Affairs leaked that Beijing hoped to revive its "Asians for Asian diplomacy" in the aftermath of its disastrous "wolf warrior" diplomatic campaigns. The sources also confirmed that the development was urgently prompted by Taiwan's domestic politics which has become increasingly hostile against China. According to recent polls, 95% of the self-ruled island's population are unwilling to cede to the Chinese Communist Party (CCP)'s claims of national rejuvenation. More Taiwanese are also calling for independence, consequently boosting the Democratic Progressive Party's popularity to have a landslide victory at the next election. Likewise, Japan too would like to talk with Beijing. It wants to see if there is a way to reduce tensions in the Taiwan Strait and the East China Sea. Various constituencies in Nagatacho and the business community want better relations between the countries, and a breakthrough would help the Suga administration (and the LDP) when the country holds national elections in the fall.

Meanwhile, an independent investigation by US experts confirmed the cyberattacks on the US-Japan joint-development programs. Lockheed Martin voiced concern that the cyberattacks could have already spread throughout MHI's computer networks, affording the threat actor unprecedented access to classified information about the F-35 joint strike fighter. The US Department of Defense and the State Department consulted Japan's Ministry of Defense and Ministry of Foreign Affairs regarding its intention to possibly undertake serious retaliatory actions against the perpetrator of the latest cyberattack.

In addition to the fact of the attack, its timing is problematic. The Pentagon is facing intense scrutiny in Congress regarding the F-35's cost and the need for an alternative management structure for international program development. For Japan, the cyberattack comes just as the country is preparing to renegotiate its status with the Pentagon to become a full-fledged partner of the fifth-generation aircraft's industrial base consortium.

The cyberattack threatens to overshadow the Closing Ceremony of the Games. Japan is confronted with the difficult choice of protecting its international reputation while navigating the evolving cyber threat landscape and balancing its own interests in lock-step with the US.

Questions for Team Japan and Team USA

As the Cybersecurity advisors to the Prime Minister/President from different government departments and ministries, use the guide questions below to formulate concrete policy recommendations to improve US-Japan cybersecurity cooperation in the aftermath of the

cyberattack.

1. Identify up to three remediation strategies that your team should undertake within the 24-36 hours following the incident.
2. Identify up to three actions that your team wants the other teams TO TAKE.

3. Identify up to three actions that your team wants the other teams NOT TO TAKE.
4. With a heightened sense of urgency, identify up to three policy recommendations that your team should pursue in close coordination with the other teams--taking into full consideration inherent characteristics such as comparative advantages and political limitations--to address the cyberattack.

Questions for Team IOC

As the Cybersecurity advisors to the President and Board Members of the IOC, use the guide questions below to arrive at policy recommendations to achieve the successful conclusion of the Tokyo 2020 Olympics and to maintain the credibility of the IOC in conducting future games in the aftermath of the cyberattack.

1. Identify up to three remediation strategies that your team should undertake within the 24-36 hours following the incident.
2. Identify up to three actions that your team wants the other teams TO TAKE.

5. Identify up to three actions that your team wants the other teams NOT TO TAKE.
6. With a heightened sense of urgency, identify up to **three policy recommendations** that Team IOC should pursue in close coordination with USA/JAPAN--taking into full consideration the need to successfully close the Olympics and other political and economic limitations--in the aftermath of the cyberattack.

Second Move

After a comprehensive technical investigation and close consultation with the Five Eyes community, the US has decided to name and shame China as the perpetrator of the cyberattack against the JOC that reached the MHI-Lockheed Martin joint-development program. According to a Five Eyes report, the Chinese-linked group, APT12—which has strong ties to the Ministry of State Security—is the primary suspect. The report explained that APT12 obtained hacking tools previously used by the GRU and reverse engineered them to launch far more sophisticated and targeted attacks on heavily-guarded F-35 joint development programs. The US and other members of the Five Eyes are eager to reach out to the EU to launch a coordinated effort to publicly attribute the attacks against the JOC and MHI to APT12.

The JOC, several Diet representatives, and the International Olympic Committee want to delay any Japanese involvement in the attribution campaign until the Olympics are over. Japanese defense officials strongly support the collective effort to call out China. The diplomatic community wants the Suga administration to distance itself from the naming and shaming campaign to avoid a diplomatic downturn as preparations for their high-level meeting with

Chinese counterparts are moving forward and a breakthrough to de-escalate tensions in the Taiwan Strait and the East China Sea seems possible.

Question for Team Japan, Team US, and Team IOC

Does this new information provided change your answers from the first move? If you have changed your answers, please be prepared to explain why in the group presentation.

1. Identify up to three remediation strategies that your team should undertake within the 24-36 hours following the incident.
2. Identify up to three actions that your team wants the other team(s) TO TAKE.
3. Identify up to three actions that your team wants the other team(s) NOT TO TAKE.
4. Identify up to three policy recommendations that your team should pursue in close coordination with the other team(s)--taking into full consideration the latest development--to address the cyberattack.