CENTER FOR
CYBERSECURITY
POLICY AND LAW

ADDRESSING INTERNATIONAL IT CONCENTRATION RISK: A FIVE-EYES INFORMED EXERCISE SEPTEMBER 2025

Compiled by:

John Banghart, *Senior Director for Cybersecurity Services*
Alex Botting, *Senior Director for Global Security and Technology Strategy*
Adam Dobell, *Director Global Security and Technology Strategy*
Tim McGiff, *Project Manager*

Abstract / Executive Summary

On April 29, 2025, adjacent to the RSA Conference 2025, the Center for Cybersecurity Policy and Law ("the Center") convened the latest in a series of multi-stakeholder tabletop exercises exploring information technology (IT) concentration risk. Over the past 18 months, the Center has led similar exercises that have directly and indirectly examined IT concentration risks.[1]

What began as an exploration of the theoretical risks that governments may be exposed to through the concentration of vendors and specific IT products and services has since grown to be an ongoing series investigating various aspects of the very tangible threat that IT concentration risk poses to governments and critical infrastructure. The exercises have taken place at a time when cybersecurity resilience is more aggressively being tested by nation-state and non-nation state actors.

This report summarizes the findings and recommendations of the RSA exercise. Previous exercises focused on how individual governments assess their concentration risk and consider guidance or policies to mitigate risks. In contrast, the purpose of this exercise was to explore IT concentration risk within a broader international context and was conducted with Five Eyes officials and industry representatives. Specifically, it was centered on exploring IT concentration risk in the context of coordinated Chinese-state actor cyber operations against a trio of fictional countries representing a Five Eyes alliance dynamic.[2]

The Five Eyes countries are uniquely positioned to lead efforts to improve the understanding of IT concentration risk and to develop common definitions, metrics, and methodologies because of their longstanding cybersecurity cooperation, robust policy and legal frameworks, and trusted information-sharing mechanisms that underpin joint decision-making and collective defense in the cyber domain.

The outcomes of the exercise informed the following recommendations:

1. An internationally trusted entity with experience in developing consensus-based standards and guidance, potentially the U.S. National Institute of Standards and Technology (NIST),

[1] *Addressing Concentration Risk in Federal IT.* https://www.centerforcybersecuritypolicy.org/insights-and-research/addressing-concentration-risk-in-federal-it
Addressing IT Concentration Risk in the Australian Government. https://www.centerforcybersecuritypolicy.org/insights-and-research/addressing-it-concentration-risk-in-the-australian-government

[2] The Five Eyes refers to a long-standing intelligence alliance between the governments of Australia, Canada, New Zealand, the United Kingdom, and the United States.

should work toward developing and promoting a common definition of IT concentration risk and a methodology or metric to measure and assess it.

2. Governments should assess the presence and associated risks of IT concentration within and across government and critical infrastructure environments, and develop policies that establish appropriate risk tolerance in various contexts. To do this effectively, governments should employ a developed and standardized definition of IT concentration risk, along with a methodology and metric to measure and evaluate it.

3. Governments should assess the potential cascading and cross-border effects of IT concentration risk. This includes effects within their own government and those of regionally proximal and geopolitically aligned governments. Particular attention should be paid to those countries with which they have dependencies in critical sectors such as defense.

- IT concentration risk should be raised and addressed at an appropriate political level in bilateral and multilateral forums among those countries that have shared dependencies in critical sectors.
- The Five Eyes governments should work together to develop and share intelligence assessments with industry, particularly critical infrastructure operators, of how adversaries - particularly nation-state actors - might exploit IT concentration to inflict cascading and cross-sector degradation of systems across their networks. This effort should leverage existing intelligence-sharing frameworks and be informed by national threat assessments, such as the Canadian Government's National Cyber Threat Assessment 2025–2026, which identifies IT concentration as a key cybersecurity trend. These shared assessments will strengthen defensive postures and resilience initiatives within the Five Eyes community and among allies.

In addition to the above recommendations, the exercise identified potential areas for further research and assessment, and raised some valuable questions that the exercise was not specifically designed to address.

This after-action report summarizes the exercise itself, provides additional guidance regarding the recommendations above, and identifies additional areas in need of further exploration. Given the growing prevalence of IT vendor concentration, we hope that the paper will spur additional efforts to assess and mitigate the associated risks, to the benefit of cybersecurity and resilience in public and private IT networks.

Exercise Background

In furtherance of the Center's mission to provide government, private industry, and civil society with practices and policies to better manage security threats, the Center engaged with public and private stakeholders in a third exercise designed to explore the issue of IT concentration risk. This particular exercise focused on government IT concentration risk in a multilateral international context. This exercise was designed to expand upon the concepts and findings of earlier exercises related to this topic, which can be found on the Center's website.[3]

The Center has expanded its conception of IT concentration risk since its initial exercise in April 2024. In particular, the Center considers IT concentration risk along both vertical and horizontal axes. A vertical risk occurs when many or all computer systems, applications, networks, etc., in the same environment share similar or identical software, configurations, or hardware. Specific examples include organizations that rely on a single provider for most or all operating systems, office productivity tools, email, chat, conference, web browsers, cloud services, security, and identity capabilities across the enterprise. Additionally, IT concentration risk can be considered a horizontal risk, as it occurs when a specific entity or IT solution is used widely across a range of organizations or environments, often with interdependencies among them.

The purpose of this exercise was to explore IT concentration risk in government environments along both the vertical and horizontal axes. In particular, it was designed to:

- Explore how various levels of concentration risk might be exploited by a sophisticated and aggressive nation-state cyber threat actor.
- How concentration risk might affect coordinated response efforts among allied governments.
- How a diverse technology ecosystem might reduce the likelihood of cascading or catastrophic cyber incidents.

Since the Center commenced this series of exercises in 2024, international governments are starting to update assessments and determine initial policy responses to IT concentration risk. For example, the Canadian Government's National Cyber Threat Assessment 2025–2026 highlights "Vendor concentration is increasing cyber vulnerability" as a key trend.[4] This trend notes that the provision of many technology services is concentrated among a few dominant providers, making them prime targets for malicious cyber activity and increasing the potential for systemic disruption across sectors — including critical infrastructure — if these vendors are compromised. This underscores

[3] Center for Cybersecurity Policy and Law. https://www.centerforcybersecuritypolicy.org/

[4] *Canadian Centre for Cyber Security: National Cyber Threat Assessment 2025–2026*. https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf

the urgency and importance of addressing IT concentration risk not just within national policy, but as a priority for international coordination and collective defense.

Australia is also demonstrating policy responsiveness to IT concentration risk. Following the Center's Canberra-based exercise in March 2025, the Australian Government integrated concentration risk as a policy priority in its *Charting New Horizons – Horizon 2 Policy Discussion Paper* (July 2025).[5] The policy discussion paper explicitly identifies IT concentration as a growing concern that could undermine access to critical cyber services in times of crisis or conflict, noting that this risk may affect sovereign cyber capability and resilience.

It calls for joint analysis by government and industry to map concentration risks, assess vulnerabilities, and identify where sovereign capabilities may need to be developed or prioritized. By directly linking concentration risk to national resilience and sovereign capability, Australia has signaled its intent to explore mitigation strategies. This mirrors the core findings of the Center's exercise and reinforces the importance of addressing risk as both a national and international policy challenge.

Since the most recent exercise at RSA 2025, there are also nascent policy initiatives underway in the United States Government, which can assist in addressing the risk, such as Executive Order 14306 of June 6, 2025, which directs updates to OMB Circular A-130. A-130 is the U.S. federal government's primary policy framework for managing information resources, including digital services, cybersecurity, privacy, and IT procurement. The updates to A-130 should incorporate new guidance on risk management and digital services procurement that addresses IT concentration risk and related resilience concerns. These evolving frameworks underscore the need for a coordinated, international approach to IT concentration risk and its implications for both domestic and collective cyber resilience.

[5] *Charting New Horizons – Horizon 2 Policy Discussion Paper.* https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/charting-new-horizons-horizon-2-policy-discussion-paper.pdf

Exercise Development & Overview

The Center developed a red team/blue team exercise around a plausible real-world scenario in which several fictional allied governments, modeled on the Five Eyes, were targeted by a fictional, sophisticated Chinese-sponsored threat actor intent on causing significant disruption without fear of attribution. The IT infrastructures of the allied governments and the capabilities of the cyber threat actor were designed to reflect real-world government infrastructures and capabilities while using fictional vendor and product names.

The exercise included an adjudication and facilitation team (FAC), an adversarial Red team representing a People's Republic of China (PRC) sponsored threat actor (ADV), and three Blue teams representing government agencies within their respective countries responsible for regulating and overseeing their respective transportation sectors.[6]

Each of the three Blue teams' IT infrastructure reflected a differing level of IT concentration risk:

- The isolated island nation of Veridia was represented by the Veridian Home Transportation Office (VHTO). Their IT infrastructure represented a high level of IT concentration characterized by extensive centralization and deep reliance on a limited set of key vendors.
- The large and landlocked nation of Eldoria was represented by the Eldorian Critical Infrastructure Management Department (ECIMD). Their IT infrastructure represented a moderate level of IT concentration characterized by a mix of centralized IT and more segmented critical systems.
- The rugged and mountainous Argonia was represented by the Argonian Transit Protection Agency (ATPA). Their IT infrastructure represented a low level of IT concentration characterized by a decentralized and diverse architecture.

In order to better facilitate an examination of the exercise's objectives, the exercise began with the initial stages of the attack already underway. The three Blue teams were aware of minor operational disruptions and anomalous network activity, and the ADV team was provided with IT environment reconnaissance and pre-positioning already achieved. Consistent with real-world incidents, in Turn Two, the ADV team would be given possession of compromised signing keys for OmniCorp-Ident, one of the major IT vendors within the scenario, and the core identity and access management suite from OmniCorp that underlies all their products and services.

While great care was taken to ensure that the exercise was reflective of a realistic, real-world scenario, it was primarily scoped to illustrate reasonable technical aspects of IT concentration risk. It was not designed to explore the nuances of government IT procurement or the complexities of

[6] Responsibilities and authorities included can be found in Appendix B.

geopolitical conflict, and the Blue teams represented simplified composites of real-world government organizations.

Exercise Summary

At the beginning of the exercise, each team was provided a brief background of their goals, available resources, and the general scope of the exercise. Gameplay was structured around four Turns, where each team was given a set number of action points (APs) to undertake tasks to achieve their goals. At the end of each Turn, the FAC team would adjudicate the results, and each team would be informed of the new game state ahead of the next Turn.

Goals

The ADV team was tasked with compromising multiple governments, with a focus on the agency most responsible for the transportation sector in the Blue teams' nations. The primary goal was to create disruption and confusion, and to demonstrate the potential for greater harm while avoiding any actions that would likely lead to kinetic military conflict. To facilitate this, the ADV team was given rules of engagement that included avoiding direct human casualties.

The three Blue teams were tasked with ensuring that mission-critical IT services remained operational, that unauthorized access to systems and data was limited, and that transportation networks within their country were functioning safely and effectively.

Gameplay: ADV

The exercise began with the ADV team engaging in a drawn-out discussion about how to achieve their goals most effectively and how to balance expending their limited APs on potential long-term payoffs versus immediate successes.

The ADV determined they should prioritize most of their APs in the first two Turns to attack the VHTO. This was informed by the high concentration of OmniCorp in the VHTO environment and the meaningful preposition against OmniCorp that the ADV team possessed, including a compromised OmniCorp-Ident signing key. During these turns, a small number of APs were used to slowly expand access to both the ECIMD and ATPA IT environments. However, the more diversified ECIMD and ATPA ecosystems necessitated more discussion about how to target them and disincentivized focused ADV efforts.

In the latter half of the exercise, having burned much of their OmniCorp access and having achieved their initial objectives against the VHTO, the ADV team turned more of its attention to operational disruptions of the ECIMD and ATPA teams. While the ADV team achieved penetration into the ECIMD and ATPA networks, it was significantly more limited than what had been achieved against the VHTO due to the more diversified IT environments and fewer resources spent in the initial turns. This resulted in the ADV team having more limited options for operational disruption.

By the end of Turn Four, the ADV team had, at various points, managed to accomplish the following through the targeting of VHTO:

- Exfiltration of satellite/GPS data.
- Exfiltration of VHTO incident response plans.
- Disruption of satellite communications.
- Disruption of maritime operational scheduling systems.
- Compromise and spreading of fake incident response communications.

By the end of Turn Four, the ADV team had, at various points, managed to accomplish the following through the targeting of ECIMD:

- Reset passwords for OmniCorp-enabled services.
- Disabled Eldorian rail switching systems.
- Wiped the security telemetry of the primary security provider.

By the end of Turn Four, the ADV team had, at various points, managed to accomplish the following through the targeting of ATPA:

- Disabled baggage handling for airports through supervisory control and data acquisition (SCADA) compromise.
- Disabled gondola transportation infrastructure.

The ADV team acknowledged early on that the less restrictive rules of engagement and the encouragement to create significant operational disruption would empower them to move quickly and focus on causing publicly noticeable damage. They embraced the tactical flexibility of burning through their compromised access quickly as long as it was in service of more disruptive effects.

Gameplay: Veridian Home Transportation Office (VHTO)

The VHTO began the exercise with the knowledge that their cybersecurity teams had detected increased probing and scanning activity originating from known state-sponsored infrastructure targeting their external network perimeters and key vendors. Initial analysis (High Confidence) indicated reconnaissance focused on enumerating and identifying vulnerabilities in software/hardware products and services used throughout the agency.

The initial incident information set the backdrop for the VHTO's first turn discussions. These discussions were heavily focused on how to prioritize information gathering and sharing activities. Participants debated the value of informing their country's cybersecurity agency, engaging with the VHTO's IT vendors, notifying Veridia's critical infrastructure owners and operators, and international outreach to allied governments. With limited APs, the VHTO team determined that informing the Veridian cybersecurity agency and engaging with their IT vendors was the most pressing.

As the exercise progressed into Turns Two and Three, the VHTO team split their resources evenly between remediating operational disruptions and continuing to gather and share information about the ongoing incident with appropriate domestic and international stakeholders. During these turns, the VHTO team discussed the potential depth of their compromise due to the high concentration of OmniCorp products, the various ways in which they might coordinate an international response to the ongoing cyber incident, and the potential disruption of critical infrastructure and transportation operations due to extensive remediation activities.

By Turn Four, the VHTO team was frustrated by their lack of progress in kicking the ADV team out of their networks and openly discussed what it would take to move off OmniCorp services to an alternative. The VHTO team refocused its APs entirely on remediation efforts as the exercise concluded.

Gameplay: Eldorian Critical Infrastructure Management Department (ECIMD)

The ECIMD began the exercise with the knowledge that their cybersecurity teams had detected increased probing and scanning activity originating from known state-sponsored infrastructure targeting their external network perimeters and key vendors. Initial analysis (High Confidence) indicated reconnaissance focused on enumerating and identifying vulnerabilities in software/hardware products and services used throughout the agency.

During Turn One, the ECIMD team focused on establishing situational awareness and preparing for a coordinated response. They directed efforts to:

- Gather more information from vendors, compromised targets, and internal stakeholders to better understand the scope of the threat.
- Convene cross-governmental actors and begin preparatory work on a formal incident response plan.
- Seek intelligence support from key international partners.

The team also explored what regulatory levers could be activated to compel cooperation from critical vendors and began to define legal authorities for emergency information gathering.

As the exercise progressed into Turns Two and Three, the ECIMD’s focus shifted to communications, containment and remediation measures, and contingency planning. Internal government and public alerts were issued, backups of critical data were created, passwords and credentials were reset, non-essential travel was shut down, and coordination with international partners was ramped up. Despite the wide-ranging efforts, operational disruptions of transportation systems continued to outpace defensive efforts.

By Turn Four, the ECIMD team was still attempting to remediate operational disruptions to transportation systems, spending APs to restore rail-switching systems and organize alternate transportation options for critical services. However, the ECIMD team also began assessing the longer-term implications of the ongoing attack and various ways in which they might prevent or minimize the effects of a similar incident in the future. The ECIMD team's actions to finish the exercise included launching a regulatory review to map vendor interdependencies and assess concentration risk across Eldoria’s government IT systems, and beginning cabinet-level conversations focused on options to diversify digital identity infrastructure and strengthen oversight over critical vendors, particularly those supplying authentication and infrastructure services.

Gameplay: Argonian Transit Protection Agency (ATPA)

The ATPA began the exercise with the knowledge that their cybersecurity teams had detected increased probing and scanning activity originating from known state-sponsored infrastructure targeting their external network perimeters and key vendors. Initial analysis (High Confidence) indicated reconnaissance focused on enumerating and identifying vulnerabilities in software/hardware products and services used throughout the agency.

After considering the initial incident information, the ATPA team spent Turn One discussing the most efficient way to gather and share information with relevant domestic and international partners while spinning up their security teams to begin remediation efforts. The ATPA team settled on notifying the Argonian cybersecurity agency and alerting the ATPA’s own security teams to begin implementing mitigations where possible.

As the exercise progressed into Turns Two and Three, the ATPA team maintained a focus on understanding and addressing their own incident. Most of their APs for these turns were spent preparing back-ups of critical systems, implementing credential resets, enabling threat hunting, and interfacing with their IT vendors. It wasn't until the end of Turn Three that any APs were spent to actively communicate with one of their allied countries, and this was prompted by fears that the VHTO’s loss of satellite communications might impact the ATPA’s own transportation networks.

At the end of Turn Four, with operational disruptions mounting, the team decided that it needed to increase engagement with its allies in the ECIMD and VHTO to understand the threat better and to coordinate a group response. The ATPA’s APs were evenly split between this new international coordination and attempting to remediate the operational disruptions at their airport and gondola infrastructure.

Findings & Recommendations

The exercise outcomes supported a number of findings related to nation-state cyber threats and information sharing that are the basis of this report's recommendations:

- **Vertical IT Concentration Risk Incentivized and Informed Attacks:** Throughout the exercise, the ADV team looked to take the path of least resistance for the greatest possible gain. The early targeting of Veridia stemmed from the assessment that their high level of vertical IT concentration would facilitate rapid progress. The reluctance to attack Argonia's diversified security IT stack and the disproportionate amount of time spent by the ADV team discussing how to achieve their goals against Eldoria and Argonia reinforced that low levels of vertical IT concentration acted as a disincentive to attacking their infrastructure, particularly at the early stages of the attack. These findings support the notion that vertical IT concentration risk does influence and incentivize certain types of cyber threat activity.

- **Information Sharing May Mitigate Horizontal IT Concentration Risk:** While the ADV team tended to avoid targeting IT entities with low levels of presence across all three target countries, they also became reluctant to attack the same IT entity across all three target countries simultaneously. The ADV team worried that information sharing between the three might increase the chance they would zero in on the attack vector and focus response efforts. While the information-sharing actions of the Blue teams within the context of this exercise were limited, the mere existence of the possibility of information sharing still had a tangible effect on the ADV team's actions.

- **Less Restrictive Rules of Engagement Amplify the Impact of Aggressive Nation State Tactics:** Despite the differing levels of concentration risk, the ADV team was largely successful in staying a step ahead of the Blue teams and created major disruptions across all three. The ADV team's success clearly benefited from rules of engagement that prioritized immediate impact over subtlety, plausible deniability, and long-term persistence. This finding raised questions about how prepared entities might be to prevent and remediate a concerted cyber operation from a sophisticated nation-state intent on causing operational disruption.

- **Addressing IT Concentration Risk Requires Preemption:** Similar to past exercises, the Blue teams found that addressing IT concentration risk during an ongoing incident was impractical due to the cost in time, resources, and the need to prioritize incident response. The exercise highlighted that if an entity is going to accept a certain level of IT concentration risk, it also needs to be prepared to mitigate incidents that exploit it.

- **Horizontal IT Concentration Risk May Affect Allied Ability to Provide Resilience and Support:** Participants noted their concern that horizontal IT concentration risk, such as a critical product or service used across allied governments, may increase the likelihood that those allies would be similarly impacted by an incident or vulnerability and may therefore be unable to provide resiliency and support. Participants raised the need to consider this aspect in national incident response plans or strategies.

Based on these findings, the Center recommends:

1. **An internationally trusted entity with experience in developing consensus-based standards and guidance, potentially the U.S. National Institute of Standards and Technology (NIST), should work toward developing and promoting a common definition of IT concentration risk and a methodology or metric to measure and assess it.**

   This exercise, like the others in this series, demonstrated that cyber threat actors benefit from high levels of IT concentration risk in their target environments. However, the full scope of what constitutes concentration risk, the ways that risk can manifest, the ways in which it may be categorized, and measurable thresholds of levels of severity remain undefined.

   The continued lack of foundational elements, such as a widely accepted definition for IT concentration risk, a methodology to assess its presence, or a metric to measure its associated risks, hinders productive discussion, limits the development of standards and best practices, and ultimately impedes efforts to effectively confront the risks associated with it.

   The Center strongly recommends that these deficiencies be addressed through an internationally trusted entity with experience in developing consensus-based standards and guidance, developing a common definition of IT concentration risk, and a methodology or metric to assess and measure it. For example, the NIST has a well-earned reputation as a good-faith partner with industry that has developed widely utilized cybersecurity guidance and frameworks like the NIST Cybersecurity Framework, NIST 800-37, and NIST 800-53r5.

2. **Governments should assess the presence and associated risks of IT concentration within and across government and critical infrastructure environments, and develop policies that establish appropriate risk tolerance in various contexts. To do this effectively, governments should employ a developed and standardized definition of IT concentration risk, along with a methodology and metric to measure and evaluate it.**

   The outcomes of this exercise support the findings of previous exercises that IT concentration risk represents a serious, underappreciated, and insufficiently understood risk to the security and resiliency of governments and critical infrastructure. As such, governments should endeavor to develop or adopt an IT concentration risk framework that includes a definition, methodology, and metrics.

Governments should use their framework to inform the development of a national strategy or policy that establishes acceptable risk tolerances in various contexts, assess current levels of IT concentration risk within and across government and critical infrastructure environments, and then recommend remedies or mitigations where necessary.

Additionally, governments may wish to consider integrating IT concentration risk considerations and requirements into government acquisition and procurement rules/regulations. This could include assessing government contractors for IT concentration risk or implementing IT concentration risk requirements for government contractors.

3. **Governments should assess the potential cascading and cross-border effects of IT concentration risk. This includes effects within their own government and those of regionally proximal and geopolitically aligned governments. Particular attention should be paid to those countries with which they have dependencies in critical sectors such as defense.**

Discussion among exercise participants highlighted the potential for IT concentration risk to have cascading and cross-border effects. As noted in the above findings, the ADV team tended to avoid targeting IT entities with low levels of presence across all three target countries, preferring to focus on IT entities whose compromise could provide access across multiple targets.

This finding suggests that governments need to consider IT concentration risk within a broader context than just their own environments. IT products and services that are used ubiquitously or that find concentrated usage among regionally proximal or geopolitically aligned governments can create horizontal IT concentration risks that may not be readily apparent.

To address this concern, IT concentration risk should be raised and addressed at an appropriate political level in bilateral and multilateral forums among those countries that have shared dependencies in critical sectors. There are many existing international security alliances and intelligence partnerships where this kind of sensitive conversation could occur.

For example, given the high level of trust and coordination that exists between the United States, Australia, and the United Kingdom, the AUKUS security partnership should serve as an appropriate forum for operational efforts of a technical or sensitive nature. It should be used as a trusted forum to continually discuss the composition of government and critical infrastructure IT environments, assessments of concentration risk across the governments, and discussions on how to ensure the diversification of critical redundancies.

Similarly, the Five Eyes governments should work together to develop and share intelligence assessments with industry, particularly critical infrastructure operators, of how adversaries—particularly nation-state actors—might exploit IT concentration to inflict cascading and cross-sector degradation of systems across their networks. This effort should leverage existing intelligence-sharing frameworks and be informed by national threat assessments, such as the Canadian Government's National Cyber Threat Assessment 2025–2026, which identifies IT concentration as a key cybersecurity trend. These shared assessments will strengthen defensive postures and resilience initiatives within the Five Eyes community and among allies.

Conclusion

This exercise brought together a mix of public and private sector participants to further explore the concept of IT concentration risk and resulted in a meaningful contribution to what we hope will be an ongoing discussion around the challenges of identifying, measuring, and mitigating IT concentration risk.

The Center and its partners recognize that this exercise and its outcomes are neither comprehensive of the issues involved nor should they be the final word on how to address them. The recommendations we put forward are meant to continue the discussion and spur new efforts that will work to improve the security and resilience of government and critical infrastructure environments.

The Center greatly appreciates the time, effort, and expertise that the planners and participants provided to the exercise and the development of this report. In particular, we want to thank the representatives of the various governments for their contributions in participating in and reviewing this report.

We look forward to continuing the discussion of the topics highlighted by this exercise.

Appendix A: Participants

The Center would like to extend our deepest thanks to the staff from the following organizations for lending their time and expertise to the exercise:

AT&T
Amazon Web Services
Australia: Department of Foreign Affairs and Trade
Australia: Department of Home Affairs
Australia: Signals Directorate
Center for Cybersecurity Policy and Law
Ciena
Crowdstrike
CyberCX
Embassy of Australia
Embassy of the United Kingdom
Forescout
FS-ISAC
Google
Google Cloud
Health-ISAC
Mastercard
New Zealand Department of the Prime Minister and Cabinet
Rapid7
Trinity Cyber
United Kingdom: Department for Science, Innovation and Technology
United Kingdom: National Cyber Security Centre
United States: Office of the National Cyber Director
United States: State Department
Venable
Zscaler

Appendix B: Exercise Summary

Gameplay was structured around four Turns, where each team implemented and/or reacted to the Actions of the other teams:

- **Turn 1**
    - Adversary (Discussion/Actions)
    - Blue/Government (Discussion/Actions)
- **Turn 2**
    - Game State (Result of the previous Turn's actions)
    - Adversary (Discussion/Actions)
    - Blue/Government (Discussion/Actions)
- **Turn 3**
    - Game State (Result of the previous Turn's actions)
    - Adversary (Discussion/Actions)
    - Blue/Government (Discussion/Actions)
- **Turn 4**
    - Game State (Result of the previous Turn's actions)
    - Adversary (Discussion/Actions)
    - Game State (Result of ADV-specific actions)
    - Blue/Government (Discussion/Actions)
    - Game State (Result of Actions / potential next steps)

Scene Setting

It is early 2026, and geopolitical instability continues throughout the world.

In the South China Sea, the state of play has stabilized somewhat as key regional countries, predominantly the Philippines and Vietnam have ceded some, not all, of their claims to China. A combination of Chinese economic coercion, diplomatic pressure, military posturing and ongoing disruption by APTs of key infrastructure has led to both countries being forced to accept a settlement. This has allowed China to further focus its efforts on Taiwan, increasing its military build-up, cyber operations and diplomatic pressure to achieve its stated objective of reunification.

On the Korean peninsula, political instability on the southern side of the 38th Parallel has led to martial law being instituted in South Korea and North Korea stepping up its information warfare campaign in an effort to stoke growing public unrest towards US forces stationed in the country. North Korea has ramped up its cybercrime (Cryptocurrency Theft and Ransomware) efforts as part of its strategy to generate revenue to support its nuclear program.

In Ukraine, tense negotiations and a tentative ceasefire continue to be punctuated by intermittent attacks and a steady stream of disruptive cyber operations by both sides. Russia has leveraged the reduced *intensity of the conflict with Ukraine to conduct increasingly significant cyber attacks against the Baltic states and Poland.*

The Five Eyes (FVEY) nations are each engaged in these conflicts to varying degrees, expending financial, military, and cybersecurity resources to enhance security within each region.

China, Russia, and North Korea, meanwhile, are increasingly coordinating through systematic intelligence sharing and coordinated efforts in cyber warfare.

The collaboration has allowed China, Russia, and North Korea to leverage each other's strengths in cyber operations, creating a more seamless, multi-faceted threat landscape. For example, China's expertise in deploying stealthy, well resourced, long-term intrusion campaigns has been combined with Russia's experience in disrupting and manipulating infrastructure to amplify the impact of these cyberattacks. By pooling their resources and intelligence, they have become more efficient at exploiting common vulnerabilities in systems, maximizing operational efficiency, and launching highly sophisticated, multi-layered attacks that are harder to defend against.

Emboldened by this new collaboration and taking advantage of domestic political divisions in FVEY countries, Chinese state-sponsored threat actors have ramped up their cybersecurity operations.

Today

In recent weeks, the cybersecurity organizations from multiple FVEY countries have issued a series of alerts and advisories regarding increasing cyber operations, attributed to state-sponsored Chinese threat actors, that are targeting a range of government agencies and critical infrastructure entities in FVEY countries, with signs of attempts to exploit vulnerabilities in both legacy and modern IT systems.

The intelligence community believes that these activities are a mixture of pre-positioning efforts and minor operational disruptions, signaling the seriousness of the threat and offering a range of strategic and tactical options should tensions escalate further. These operations coincide with heightened geopolitical tensions in the Taiwan Strait. As China's stance on Taiwan grows more assertive, the timing of these cyber activities may be seen as part of a broader effort to destabilize key infrastructure in FVEY countries in anticipation of potential regional conflict.

Teams

- Facilitators (FAC): This group was responsible for coordinating all activities of the exercise, including:
  - Guiding the other teams on background, gameplay, rules, and expectations.
  - Adjudicating all actions and requests received by the teams at the end of each turn.
  - Providing updates, responses, and injects to the teams as needed for each turn.
- Adversary (ADV): This group represented a People's Republic of China (PRC) sponsored threat actor directed to compromise multiple governments, with a focus on the agency most

responsible for the transportation sector in that nation. Primary goals are to create disruption and confusion and to demonstrate the potential for greater harm while avoiding any actions that would likely lead to open warfare or that may lead to direct human casualties.

- Veridian Home Transportation Office (VHTO): This group was responsible for regulating and overseeing the Transportation Sector of Veridia. This includes air traffic control, GPS governance, satellite regulation (licensing and oversight of commercial satellites), unmanned and autonomous systems governance and oversight, maritime enforcement and readiness, and overland security and preparedness (rail and roadways).
    - **Key data sets:** Supply delivery schedules and contents through major ports, personnel records for port security and logistics personnel, emergency response/disaster recovery plans, unclassified security plans (personnel shift schedules, software/hardware maintenance schedules, and upgrade deployments), satellite deployment and positioning information.
- Eldorian Critical Infrastructure Management Department (ECIMD): This group was responsible for regulating and overseeing the Transportation Sector of Eldoria. This includes air traffic control, GPS governance, satellite regulation (licensing and oversight of commercial satellites), unmanned and autonomous systems governance and oversight, maritime enforcement and readiness, and overland security and preparedness (rail and roadways).
    - **Key data sets:** Supply delivery schedules and contents through major rail hubs, personnel records for rail hub security and logistics personnel, emergency response/disaster recovery plans, unclassified security plans (personnel shift schedules, software/hardware maintenance schedules, and upgrade deployments), satellite deployment and positioning information.
- Argonian Transit Protection Agency (ATPA): This group was responsible for regulating and overseeing the Transportation Sector of Argonia. This includes air traffic control, GPS governance, satellite regulation (licensing and oversight of commercial satellites), unmanned and autonomous systems governance and oversight, maritime enforcement and readiness, and overland security and preparedness (rail and roadways).
    - **Key data sets:** supply delivery schedules and contents through major airports, personnel records for airport security and logistics personnel, emergency response/disaster recovery plans, unclassified security plans (personnel shift schedules, software/hardware maintenance schedules, and upgrade deployments), satellite deployment and positioning information.

IT Environment

The following fictitious companies provided the stated products and services to the VHTO, ECIMD, and ATPA teams. The indicated products and services implemented at each team were considered acceptable targets for the ADV team:

Company	**Product(s)**
BestDeviceCompany	ICT components for electrical generation and transmission.
OmniCorp	Comprehensive and integrated ecosystem of solutions tied together by a shared identity system.
OtherCompany	Popular identity and access management solution with integrations into many ecosystems.
Purple Bonnet	Linux distribution with both significant open source and corporate support options.
WebCorp	SaaS applications, specializing in communications and office productivity.
MegaCorp	Specialized cloud services to U.S. government customers.
SecuroTech	Comprehensive security tools and services.
SuperSecurity	Security tools and services.

Appendix C: Center for Cybersecurity Policy & Law

The Center for Cybersecurity Policy and Law is a nonprofit 501(c)(6) organization that develops, advances, and promotes best practices and educational opportunities among cybersecurity professionals. The Center provides a forum for thought leadership for the benefit of those in the industry, including members of civil society and government entities in the area of cybersecurity and related technology policy. The Center seeks to leverage the experience of leaders in the field to ensure a robust marketplace for cybersecurity technologies that will encourage professionals, companies, and groups of all sizes to take steps to improve their cybersecurity practices.

To learn more about the Center and our wide-ranging initiatives, please visit https://centerforcybersecuritypolicy.org.