3.6. Shield 6 : Strong region and global leadership

Focus area 1 : Continuing to use all arms of statecraft to deter and impose costs on state and non-state malicious cyber actors

Question(s) to consider:

46. Do you view attributions, advisories and sanctions as effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?

- France is determined to curb the development of cyberthreat and to that end, will use all available means at its disposal (legal, technical, diplomatic, military and economic) to raise the costs for state-sponsored and non-state malicious cyber actors. Attributions, advisories and sanctions are part of the resources available to the political authority, which France is determined to use more systematically, including at the European level (through the EU cyberdiplomatic toolbox). This is why on April, 29 for the first time, France publicly attributed cyberattacks conducted by the threat actor APT28 to the Russian military intelligence service, the GRU.
- France's current doctrine for attribution was established in 2020 by the French Cyber Security Agency (ANSS), the Cyberdefense Command (COMCYBER), the Ministry of Justice, the Ministry for Europe and Foreign Affairs, the General Directorate for Internal Security (DGSI), the Directorate General for External Security (DGSE), in accordance with the mandate they received from the Cyber crises coordination centre (C4). The C4 is an inter-agency body in charge of the cyber threat analysis and information sharing among its participants. The C4 is led by the ANSSI and meets at a technical level (C4 TECHOPS) with the DGSE, the DGSI and the COMCYBER and Directorate General of Armament (DGA). The C4 also meet at a strategic level (C4 STRAT) with the MEAE and the CNRLT. Depending on the needs, the Ministry of Justice and the French Treasury can also be invited to participate. The doctrine provides a comprehensive framework of definitions, methods that can be used to identify an attacker and a process from identification to attribution, including when the proposed attribution comes from a foreign partner.
- We share the idea that coordination is much needed to counter growing malicious cyber activity, especially through coordinated responses, be they political, economic or diplomatic. We are looking forward to strengthening our coordination in this regard, including to reach out to countries in the Pacific and Southeast Asia to raise awareness against those malicious actors and raise more support for such action.

Focus area 2 : Strengthening cyber resilience and cooperation on critical technologies in the region and reinforcing Australia's partner of choice status

Question(s) to consider:

47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?

- The Pacific and Southeast Asia are likely to be subject to an increasing digital and cyber divide between rising regional and global digital powers and smaller players which struggle to

develop capability on their own. Countries in these regions are likely to increasingly suffer from cyberattacks, for lucrative or destabilizing purposes. The resilience of these societies could be put under high pressure if they do not benefit from cyber capacity building programs in line with a free, open, secure, stable and non-fragmented cyberspace. Australia's cyber capacity building efforts play an important role to support the resilience of these regions.

- Pacific and Southeast Asia countries will likely be put under growing pressure in the global Sino-American technological competition. Partners active in the region, such as Australia or France, have a role to play to back the development of sovereign national capabilities in a region increasingly marked by geopolitical rivalries. We have also a duty to name malicious actors to inform and raise awareness on state and non-state cyber threats.

- At the same time, France expresses concerns with regards to the acquisition of commercial cyber intrusion capabilities via grey channels and cases of irresponsible use. The commercialization of cyber arms by a wide range of private actors to a growing number of state and non-state actors in the region could increase the risks for human rights and fundamental freedoms, as well as impacts to our national security and cyberspace stability. Hence the need to strengthen cooperation with partners in the region to curb the proliferation and irresponsible use of CCICs.

48. Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?

Focus area 3 : Continuing to shape, uphold and defend international cyber rules norms and standards in our interests

Question(s) to consider:

49. In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?

- France welcomes the adoption of the final report of the Open-Ended Working Group on ICT security in the UN at the beginning of July, in close cooperation with Australia. Australia could continue promoting an action-oriented, cross-cutting and multi-stakeholder approach within the Global Mechanism, in order for it to be as efficient, useful and inclusive as possible for all States. Australia could also keep promoting the necessity to advance the implementation of the normative framework for responsible State behaviour among countries from the Indo-Pacific region by continuing to engage with them on that topic.

- As an example, Australia could actively participate in cross-regional initiatives aiming at implementing specific norms. France has been committed to implementing the UN framework for responsible State behavior, notably, together with the United Kingdom, through the Pall Mall Process, to which Australian contributions have been valued. We encourage Australia to continue to engage with this initiative and to participate in its global promotion.

- As another example, as an important global donor, Australia could continue to support cyber capacity building programs to ensure the understanding and implementation of certain norms of responsible behaviour in cyberspace, for instance throughout programs dedicated to the implementation of due diligence requirements. The Pacific Islands Forum could be a useful forum in that perspective.

- As confidence building measures are one of the pillars of international cooperation in the cyber field, Australia could also continue promoting the implementation of the confidence building measures agreed at the international, regional and bilateral levels.
- ANSSI places great important on its participation in the Pacific Cyber Security Operational Network. The continuous investment from Australia in this initiative is necessary to strengthen cyber capabilities across this strategic area.

Focus area 4 : Driving a program of international regulatory alignment and enhancing regional cyber policy and regulatory capacity

Question(s) to consider:

50. What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?

- To enhance cyber regulatory alignment, there is a need to contribute to international actions aiming at implementing the UN normative framework. For instance, the Pall Mall Process, an international and multistakeholder initiative aiming at curbing the proliferation and irresponsible use of commercial cyber intrusion capabilities (CCICs) in the wake of norm 13(i) and the "non-proliferation" principle of the 2018 Paris Call for Trust and Security in Cyberspace, has highlighted policy voluntary recommendations for States and industry to limit the risks associated with the he development, facilitation, purchase, and use of such capabilities. France sees this forum as a way to build common understanding on the methods to uphold the UN normative framework, with a view to curb a growing threat to our national security, human rights and fundamental freedoms while improving trust, security and stability in cyberspace.

- Beyond *soft law* standards, France actively contributes to the development of the EU regulations to improve the cybersecurity of products and critical infrastructure, as well as the EU readiness and solidarity in cyberspace. The requirements set out in the NIS 2 directive (EU), but also the *Cybersecurity Act*, the *Cyber Resilience Act* and the *Cybersolidarity Act*, play a major role in building safer technology, world-class protection for critical infrastructure and a resilient economy at the digital age. The EU regulatory strategy, coupled with important investments for innovation, could be viewed as similar to the Australian's "cyber shields" vision.

- Complementary to this twofold approach, France encourages leading cyber partners such as Australia to contribute to international open-source solutions which contributes to build safer cyberspace. As an example, the EU has launched in May 2025 the EU Vulnerability Database (EUVD) to signal and patch critical vulnerabilities.