INFORMATION NOTE FOR THE DEPUTY MINISTER AND CHIEF OF THE DEFENCE STAFF - US CYBERSPACE SOLARIUM COMMISSION FINAL REPORT / NOTE D'INFORMATION POUR LA SOUS-MINISTRE ET LE CHEF D'ETAT-MAJOR DE LA DEFENSE - LE RAPPORT FINAL DE LA COMMISSION SOLARIUM DE CYBERESPACE DES ETAS UNIS

KEY MESSAGES

- The Cyberspace Solarium Commission (CSC), a bipartisan group established by the United States Congress in 2019, released its final report on 11 March 2020, recommending a new "whole of nation" cyber strategy for the United States.

- The CSC advocates a strategic approach of "layered cyber deterrence", with the aim of reducing the "probability and impact of cyber-attacks of significant consequence". The report also adopts the Department of Defense concept of "defend forward" as a national strategy for security cyberspace using all of the instruments of power, including military power.

- The shift towards defend forward as a whole-of-nation approach comprised of diplomatic, economic, regulatory, legislative, and military instruments to secure and defend national interests in cyberspace is a signal that the US may expect more of allies and partners. For Canada, this may mean more demand for intelligence sharing among the Five Eyes and enhanced capacity to conduct active cyber operations in defence of strategic interests or in support of military activities.

BACKGROUND

- In 2019, the United States Congress established the Cyberspace Solarium Commission as a bi-partisan, intergovernmental, and multisector group tasked with examining the US' ability to counter attacks of "significant consequences" and develop a "consensus on a strategic approach to defending the US in cyberspace".

- Co-chaired by Senator Angus King (I-ME) and Representative Mike Gallagher (R-WI), the Commission undertook an extensive program of work over the course of nine months, including a research phase comprised of more than 200 key expert interviews, and a deliberation phase focused on synthesis and development of recommendations. The Commission was modeled after the original 'Project Solarium' launched by President Eisenhower in 1953 to develop a long-term counter-USSR strategy in the early days of the Cold War.

- The Commission's final report was released publicly on 11 March 2020, and includes a range of recommendations aimed at reforming government organization and structures, promoting cyber resilience, and ensuring greater unity of effort between the US Government and private sector in cyberspace.

LAYERED DETERRENCE

- Building upon the Department of Defense's (DoD) 2018 Cyber Strategy, which prioritizes persistent cyber engagement under the threshold of armed conflict, the Commission takes the position that deterrence is possible in cyberspace, using a range of instruments of national power. It advocates a strategic approach of "layered cyber deterrence" combining "enhanced resilience

with enhanced attribution capabilities and a clearer signalling strategy with collective action by our partners and allies".

- While deterrence has been a long-standing element of US strategies across all domains, layered cyber deterrence differs from past emphasis on deterrence by threat of punishment, prioritizing instead deterrence by denial, reducing vulnerabilities, and increasing resilience through stronger public-private collaboration.

- Layered cyber deterrence is comprised of three elements:
    - Working with allies and partners to dissuade adversaries from using cyberspace to undermine national interests through **norms of responsible state behaviour**;
    - Securing critical networks and building public and private sector resilience to **deny benefits** to adversaries; and
    - **Imposing costs** to deter future malicious behaviour and reduce ongoing adversary activities short of armed conflict through the employment of all instruments of power, including military power.

- Of particular interest to Defence, the Commission adopted the DoD concept of defend forward – a key component of US Cyber Command's Persistent Engagement Strategy that aims to disrupt and defeat (rather than prevent) malicious cyber activities. While the notion of defend forward may seem, at first glance, to sit somewhat uncomfortably within a deterrence framework which is aimed at preventing such activities, it appears to be a deliberate attempt to shift the policy and operational narrative in the US.

- The CSC report specifies that the US should adopt defend forward as a national strategy, while clarifying that it is an inherently defensive strategy, even if it has offensive components at operational and tactical levels. Nevertheless, differences in terminology aside, the Solarium report retains space for the incorporation of pre-emptive military activity across the spectrum, from competition to under-the-threshold operations against adversaries in cyberspace.

POLICY PILLARS AND RECOMMENDATIONS

- The report consists of more than 75 recommendations that are organized into six policy pillars.

1. **Government Reform**: The report found that the government's decentralized approach to cyber issues has not kept up with how cyberspace has transformed every aspect of American life, and recommends reforms to the US government's structure and organization for cyberspace, including:
    a) The development of a national cyber strategy that embraces layered deterrence and empowers cyber agencies including the Cybersecurity and Infrastructure Security Agency (CISA) (the US equivalent to Canada's Centre for Cyber Security), including through increased authorities and funding;
    b) The establishment of House and Senate committees on cybersecurity to provide integrated oversight of the cybersecurity efforts dispersed across the federal government;

c) The establishment of a National Cyber Director within the Executive Office of the President, as the principal advisor for cybersecurity-related issues and to lead national-level coordination of cybersecurity strategy and policy.

- On the recommendation to create a national cyber strategy, the report goes into considerable detail on the need to develop a multi-tiered signaling strategy aimed at altering adversaries' decision calculus and addressing risks of escalation (which some have argued is increased by persistent engagement). It argues that "the strategic level of signaling should involve overt, public diplomatic signaling through traditional means", as well as "clandestine, protected, and covert signaling (including through non-cyber means)" that is deliberately coupled with cyber operations.

2. **Strengthen Norms**: The report makes several recommendations to further the promotion of responsible behaviour in cyberspace and the strengthening of international norms, including through the creation of a new Bureau of Cyberspace and Emerging Technologies to lead US government efforts to develop and reinforce norms; active engagement in international fora on information and communications technology standards; and improving international tools for law enforcement.

3. **Promote National Resilience**: To ensure that the public and private sectors are capable of responding to, and recovering from, cyber-attacks, the report recommends that Congress create a "cyber state of distress", accompanied by a dedicated cyber response and recovery fund, and a Continuity of the Economy plan, to promote national resilience.

4. **Reshape the Cyber Ecosystem**: The CSC acknowledges that steps must be taken to reshape the cyber ecosystem towards greater security, including through the development of an industrial base strategy for information and communications technology (ICT) to protect trusted supply chains; investment in Research and Development in emerging technologies; and contesting efforts by China to corner the global market and set standards in technologies such as 5G. The report also suggests legislation on national data security and privacy on the premise that private data can be used for nefarious purposes, thus linking data security and national security.

5. **Operationalization Collaboration with Private Sector**: The Commission recognizes that in cyberspace, the government is often not the primary actor nor does it hold responsibility for the defence and security of critical infrastructure and networks. Accordingly, the CSC calls for the operationalization of cybersecurity collaboration with the private sector.

6. **Preserve and Employ the Military Instrument of Power**: Finally, the report emphasizes the importance of imposing costs to deter future malicious behaviour and reduce ongoing malicious cyber activities below the threshold of armed conflict through the employment of all instruments of power.

   - A key element of cost imposition is the "military instrument of power". The report recommends that the Department of Defense (DoD) conduct a force structure assessment of the Cyber Mission Force, as well as a cybersecurity vulnerability assessment of critical weapons systems. DoD should also conduct a study on amendments to the Standing Rules of Engagement and Standing Rules for Use of Force for U.S. forces to address the unique aspects of conducting modern military operations in cyberspace, and review the

delegation of authorities, including for information operations, to better enable the use of offensive cyber operations.

- The Report also suggests a mandatory requirement for the DoD to define its reporting metrics (i.e. how it measures success) for its persistent engagement strategy. This is to respond to criticisms that the new military posture in cyberspace favours activity – measured by the number of operations – that may be divorced from broader strategic goals.

POTENTIAL IMPLICATIONS FOR CANADA

- The report was, unfortunately, released publicly just as global attention began to turn to the coronavirus pandemic, and it is therefore difficult to assess at this time Congress' disposition towards the Commission's ambitious suite of legislative and investment recommendations. However, if implemented, there are potential areas for enhanced cooperation with the US that Canada should track closely in the coming months, such as:

  a) Collaboration at the diplomatic level on reinforcement of international norms and the development of standards, including through bilateral and multilateral fora such as the International Telecommunications Union.

  b) Sharing of best practices on the recruitment, training, and retention of cyber-smart individuals, including through partnerships with the private sector, to bolster capacity to plan and execute cyber military activities; and

  c) Coordination on the development and implementation of an ICT industrial base strategy to protect the integrity of interconnected supply chains. On this point, it is possible that Canada's eventual decision on 5G may have an impact on the potential for cooperation on ICT issues, including those that relate to resilience of the Defence Industrial Base.

- The report recommends greater attention be paid to preparedness planning and exercises to refine response mechanisms and processes, including the establishment of a biennial National Cyber Tabletop Exercise, with senior level participation from across government and private sector, as well as international partners. There may be opportunities for Canadian participation in these exercises, if implemented.

- From the defence lens, the Commission's adoption of defend forward as a national strategy for securing cyberspace using all of the instruments of state power, including military power, is especially significant. At the operational and tactical levels, defend forward "requires operating in allied and partner cyberspace" to implement activities such as hunting forward on allied and partner networks, deceptive countermeasures, and early warning. As Canada rolls out its active cyber capabilities in support of military operations,

  there may be new opportunities to work more closely with US Cyber Forces in the conduct of these activities.

- The report highlights the importance of international partnerships to address cyber challenges, including reinforcement of norms of responsible state behaviour, and the need for greater information sharing about cross-border cyber threats. From the defence perspective, the Commission recommends that DoD and the US intelligence community enhance collaboration with Five Eyes allies on strengthening the signals intelligence architecture to increase the scale of the available shared infrastructure that can support combined military (and not just SIGINT) operations, and leverage the unique capabilities of allies in the conduct of operations and missions.

CONCLUSION

- Through its study, the Solarium Commission has highlighted the strategic dilemma between rapid advancement in technological capabilities and enhanced connectivity, and the challenge of securing and defending critical systems, networks, and infrastructure. In recommending the adoption of defend forward as a national strategy across sectors, the Commission has signaled to US decision-makers and international allies and partners that more needs to be done, including through enhancing the military instruments of power, to deter adversaries who seek competition through cyberspace below the threshold of armed conflict.

- Canada's *Strong, Secure, Engaged* defence policy similarly highlights the need to capitalize on new opportunities to wield strategic influence and deliver operational effects in cyberspace. While DND/CAF continues to work with CSE to develop its capacity to conduct active cyber operations, increased attention to cyber challenges in the US may continue to put pressure on Canada to implement its new authorities, including those under the *CSE Act*, and capabilities for active cyber operations as part of our contribution to allied missions and activities. In the near term, it will be imperative for DND/CAF and CSE to continue to explore ways to maximise the active cyber effects afforded by these new authorities and to position ourselves to achieve 'persistent engagement' against adversaries in cyberspace, beyond the parameters of named operations and in accordance with international norms and laws.

Prepared by: Rebecca Berthiaume, D DT Pol, 613-851-6876
Consulted: Alex Seguin, D Strat A; Amy Fallis and LCol Brennan Cornell, DG Cyber
Reviewed by: Ryder McKeown, D/Dir D DT Pol,
Approved by: Kim Rebenchuk, Dir D DT Pol,
Responsible Director General: Jon Quinn, DG Contl Def Pol,
Responsible Group Principal: Peter Hammerschmidt, ADM(Pol),
Date: 27 March 2020