Feb 10

UNCLASSIFIED

MEMORANDUM FOR THE NATIONAL SECURITY AND INTELLIGENCE ADVISOR TO THE PRIME MINISTER

MEETING WITH THE CANADIAN HIGH COMMISSIONER TO THE UNITED KINGDOM ON BILATERAL COLLABORATION

(Meeting)

SUMMARY

- Public Safety Canada (PS) is convening a meeting of Deputy Ministers (DMs) with the Canadian High Commissioner to the United Kingdom (UK), Ralph Goodale on February 14, 2022. The purpose of the meeting is to discuss the High Commissioner's recent proposal of initiatives to strengthen Canada-UK collaboration on national security issues (**Tab B**).

- PS has drafted a proposal for consideration, with areas of potential focus as well as possible next steps (**Tab C**). There are significant implications for the Privy Council Office (PCO) associated with these, including the potential roles of the Interim Clerk and the NSIA. PS has also compiled a draft inventory of existing collaboration (**Tab D**).

- Separately, but related, PCO S&I has been leading work to respond to interest in increasing bilateral engagement with the United States (US) around economic security and emerging technology, stemming from recent discussions with Tarun Chhabra from the US National Security Council (NSC).

- Memory joggers are enclosed (**Tab A**).

Background

- On November 19, 2021, the Canadian High Commissioner to the UK, Ralph Goodale, contacted the Clerk of the Privy Council as well as various DMs to propose initiatives to strengthen Canada-UK collaboration on national security issues (**Tab B**). The proposal outlines thirteen areas where Canada could enhance bilateral

cooperation with the UK on security, innovation and resilience. These draw heavily from the MacDonald-Laurier Institute's paper "Evolving the Five Eyes" (**Tab E**). The proposals are categorized by six areas of work:

- Economic security and resilience;
- Military-Military Cooperation;
- Cyber Security/Operations
- National Security Communications
- Technology and Innovation
- Hostile State Activity

- PS has been leading a response to this proposal and created a draft inventory of existing bilateral initiatives with the UK (**Tab D**). The aim of the document is to inform discussion on whether there are gaps, or areas where Canada may wish to ramp up existing cooperation. PS also solicited input from departments on the High Commissioner's proposal but received limited feedback.

- Following an initial discussion among Deputies in December 2021, the Interim Clerk, Acting NSIA and the Prime Minister's Office (PMO) discussed this proposal with the High Commissioner in early January 2022. We understand the High commissioner's proposal was received favourably and that he was informed the Deputy Minister of Public Safety had been asked to move this initiative forward with other implicated Deputies.

- PS has developed a proposal for consideration (**Tab C**). This proposal is focussed around a national security strategic dialogue and four priority topics:
  - Foreign interference;
  - Economic security;
  - Societal resilience & trust; and,
  - Emerging technology and cyber values.

- Of particular note, PS' proposal envisions substantive roles for the NSIA, and potentially a role for the Interim Clerk in launching such a dialogue. This includes the potential for regular bilateral discussions between the NSIA and UK's National Security Advisor and a call between the Interim Clerk and UK Cabinet Secretary to formally establish the strategic dialogue.

- Separately, PCO S&I has been leading engagement to respond to interest in collaboration around economic security and emerging technology raised at recent meetings with Tarun Chhabra, Senior Director and Special Assistant to the President for Technology and National Security at the US NSC at the ADM level. Given that many of

the proposed initiatives put forward by High Commissioner Goodale for increased collaboration with the UK are Five Eyes in nature and touch upon economic security and/or emerging technology, it will be important to ensure coordination between the UK and US responses, and consider how to best leverage any related initiatives to maximize efforts.

- Led by PCO Plans & Priorities, work is also underway to host the next meeting of the Canada-UK Public Policy Forum in the coming months (specific date to be confirmed). This would be the second meeting following the launch between Prime Ministers in 2017. The goal is to expand and enhance Canada-UK relations across a wide range of public policy issues. While scoping is still underway, national security could be one area of focus.

Considerations

- It is clear from both PS' work on responding to the High Commissioner Goodale and PCO S&I's work on the US that there is a great deal of ongoing collaboration in the national security space between Canada and these two Five Eyes partners. However, with demand from allies for increased collaboration, it will be important to consider: whether we are making the right linkages across the fora in which we are engaged (i.e. from analytical work to policy; between innovation and national security initiatives, etc.); where Canada's national interests would be best served by increased engagement; and, where Canada could add meaningful value.

- In terms of next steps for a strategic dialogue, while PCO could play a role in launching and advancing such an effort, the substance of such discussions will require significant leadership and input from various departments and agencies. Currently, PS' proposal is very high level. Clear objectives for a dialogue would also need to be identified and refined and has implications for a wide range of departments and agencies.

  - It is notable that the High Commissioner's proposal cautions that Canada should be prepared to put something forward in order to advance bilateral collaboration. To this end, it will be imperative to move beyond very high level themes and to be prepared to discuss concrete policy or other initiatives to bring forward.

  - The UK has made significant strides by articulating a cohesive and tangible vision in *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy*. Among other things, the Integrated Review foresees the UK becoming a science and technology superpower by 2030, and

seeks to support this goal through initiatives that will maintain access to human and natural resources, advances on economic security, protecting its critical infrastructure and sensitive technologies, and a new cyber security strategy, which it recently published and which it signalled in the Integrated Review.

- It will be important to ensure coordination between the UK and US responses, and consider how to best leverage any related initiatives to maximize efforts as well as deconflict with other efforts, such as reinvigorating the Five Eyes National Security Advisors dialogue.

- In terms of next steps on this initiative, you may wish to express PCO's support in its launch, but look to PS and Global Affairs Canada to drive work forward on refining objectives and deliverables.

Mike MacDonald

Attachments

10009879

TAB A
Onglet

ANNEX B

Canada, the UK and the Five Eyes
Opportunities for enhancing collaboration on security, innovation and resilience

Possible proposals: [redacted] there are a number of such initiatives that could be considered for future discussion. What follows is a menu of options that might be drawn from:

Economic Security and Resilience

- **International Pact against Coercive Measures** – building on GAC's related White Paper, the FVEYs could collectively but unofficially champion an international "defensive pact" among liberal market economies that could deter the use of coercive economic measures with the promise of collective action.

- **FVEYs Heads of Investment Screening Bodies Meeting** – The FVEYs could consider convening an annual meeting where authorities responsible for investment screening on national security grounds meet to encourage collaboration and share best practices.

- **Creation of national security "white lists" across the FVEYs** – The FVEYs countries could jointly develop standardized clearance and vetting procedures to "clear" companies and research institutes for work in sensitive/dual-use collaborative projects. This could facilitate competition in emerging technology within "safe" parameters and incentivize companies and universities to take appropriate action to safeguard intellectual property and take security matters seriously. "Black lists" of companies, entities and institutes with links to hostile foreign governments could be maintained.

- **Supply Chain Alliance** – The UK and Canada could examine ways to map out and cross reference supply chain vulnerabilities across the FVEYs and ensure that, collectively, we are not vulnerable to supply chain disruptions due to natural or geopolitical disruption from one part of the world. Such an alliance would include for the reciprocal provision of key goods/materials among the FVEYs in times of crisis. There are a number of supply chain resilience initiatives already in existence, such of the Quad 5G and semiconductors agreement and the *Resilience Initiative* that the FVEYs could emulate or join.

Military-Military Cooperation

- Arctic Cooperation – In 2021 we have seen the European Union, United States Navy & Army publish Arctic strategies and [redacted] This presents an opportunity for Canada to engage the UK, and other like-minded partners, in finding shared avenues of collaboration in this space, and possibly to influence the trajectory of those strategies in line with Canadian interests. A shared vision of Arctic, or near Arctic (Blue Arctic), challenges combined with a desire to better align like-minded Arctic strategies could lead to concrete collaborative projects, including S&T / capability development or joints efforts in the areas of remote sensing and maritime domain awareness. Given the UK's focus on the Arctic

ANNEX B

domain at present, Canada can leverage its domain expertise to balance other areas of the bilateral defence relationship where the UK has clear advantages.

Cyber Security/Operations

- **Develop a FVEYs Cyber Warfare Collaboration Centre** – The FVEYs could consider the creation of a joint cyber training and collaboration centre to share capabilities and train the cyber forces of tomorrow.

National Security Communications

- **FVEYs International Security Communications Collective** – In light of the threat of state-backed disinformation campaigns, foreign propaganda efforts, and distortions in the perceptions of the FVEYs and liberal democracies more broadly, a more formal mechanism involving coordinated strategic communications approaches to address the information war that is already being waged against the West could be an effective response to adversaries. The group could also act as a "core group" in the Counter Foreign Interference Summit process. Allies could share strategic information on known propaganda campaigns and best practices on ways to counter such efforts.

Technology and innovation

- **Emerging technology research alliance** – In light of new and ongoing restrictions related to espionage activities of hostile states, a research alliance could facilitate the free flow of scientific knowledge on key strategic emerging technologies within the FVEYs grouping in order to maintain strategic advantage in emerging disruptive technologies including A.I., cyber, quantum computing and advanced materials science.

- **Five Eyes Tech Centre** – Take promising technology from the private sector/academia and provide a venue for collaborative projects using specific technologies.

- **Leverage the National Technology Industrial Base (NTIB)** – Canada and the UK could examine ways that the existing NTIB structure could be used to protect our collective national interests more effectively and meet the challenges of the 21st century. The NTIB is a "four eyes" US, UK, CAN, AUS framework comprising the people and organizations engaged in national security and dual-use research and development. This could include the creation of a NTIB secretariat.

Hostile State Activity

- **FVEYs framework for countering foreign interference in the university/research sector** – An agreed common framework that aims to recognize the shared threat of foreign interference on campus, agree to a common set of definitions, outlines the scope of information sharing between countries on foreign interference at universities and research institutes. Such an effort could recommend that countries align domestic frameworks with one another, agree on the scope of strategic sectors that should be protected on the grounds of national interest/national security as they related to research collaboration, monitor research collaboration in strategic

ANNEX B

sectors and identify national contact points for foreign interference on campus. (A detailed proposal developed by ILO can be found as a classified annex)

- **FVEYs Intelligence Fusion Centre on HASA** – The fusion centre would act as an intelligence hub for joint analysis of threats related to hostile state operations and interference, but also an advocacy and communications hub for disseminating information to like-minded partners such as France, Germany, Japan and South Korea.

- **FVEYs counter foreign interference project** – the FVEYs intelligence agencies, home affairs agencies and foreign ministries could collaborate to produce a review of Russian and Chinese interference activities. Findings could inform collective countermeasures, inform policy-making and even be shared with like-minded partners in Europe and Asia as appropriate.

TAB B
Onglet

Enhanced Canada-UK National Security Collaboration

Background

- On November 19, 2021, High Commissioner (HC) Ralph Goodale sent a message to national security Deputy Ministers to propose enhanced Canada-UK cooperation on national security issues.
- The interim Clerk of the Privy Council met with HC Goodale in January 2022 to discuss this initiative and potential next steps.
- On February 7, 2022, DMs from the national security community will discuss areas of focus for enhanced Canada-UK collaboration with HC Goodale.

Considerations

- Mandate letters highlighted the importance of collaborative work with like-minded countries. Priorities include building international resilience, supporting democracy and human rights, and the protection of research and intellectual property.
- In March 2021, the UK published its Integrated Review of Security, Defence, Development and Foreign Policy, which highlighted the importance of building alliances and strengthening bilateral ties with like-minded countries beyond the European Union. Canada is mentioned as a "force for good" partner.

Enhanced Strategic Coordination

Canada and the UK collaborate on national security issues in global fora, including through their membership in the Five Eyes alliance. This multilateral engagement, as well as wide-ranging activities at the bilateral level, could benefit from enhanced strategic coordination among high-level officials.

With evolving threats from state and non-state actors, Canada and the UK could explore options for a national security strategic dialogue. Potentially led by Canada's NSIA and the UK's NSA, this would allow for more frequent and formalized exchanges that would facilitate more effective responses to common threats.

Priority Topics

The following issues are proposed for further discussion with the UK:

- **Foreign Interference,** as enhanced collaboration would help prevent, identify, mitigate and respond to foreign interference domestically. Internationally, enhanced Canada-UK collaboration could bolster multilateral action against foreign interference practices from certain countries.
- **Economic Security,** with a specific focus on strengthening the research security culture of academic institutions and private sector organizations as well as protecting global supply chains (semiconductors, critical minerals, energy) to ensure safe and reliable procurement.

- **Societal Resilience and Trust,** to find solutions to prevent the erosion of public trust in national security that hampers the government's ability to establish relationships with various communities, and which can also affect the prevention of violent extremism.
- **Emerging Technology and Cyber Values,** to jointly develop frameworks to guide the use of these technologies to prevent illegal activities, while ensuring the protection of human rights, privacy and ethical considerations. Of particular interest: social media, artificial intelligence, encryption and quantum computing.

Possible Next Steps

In early January, the Interim Clerk of the Privy Council met with High Commissioner Goodale to discuss his recent letter. Possible next steps to suggest for continuing a potential Canada-UK strategic dialogue on national security include:

- A call between the Interim Clerk of the Privy Council and the UK Cabinet Secretary to formally establish the strategic dialogue.
- Regular discussions (twice yearly) between Canada's NSIA and the UK's NSA to provide overall direction to the strategic dialogue.
- Possible interaction between DMNS and its UK equivalent (National Security Council Officials – "NSCO") to discuss high-level NS policy questions of mutual concern.
- Regular meetings of DG-level working group to develop a roadmap and deliverables for the four key national security issues.

Enhanced Canada-UK National Security Collaboration

Background

- On November 19, 2021, High Commissioner (HC) Ralph Goodale sent a message to national security Deputy Ministers to propose enhanced Canada-UK cooperation on national security issues.
- The interim Clerk of the Privy Council met with HC Goodale in January 2022 to discuss this initiative and potential next steps.
- On February 7, 2022, DMs from the national security community will discuss areas of focus for enhanced Canada-UK collaboration with HC Goodale.

Considerations

- Mandate letters highlighted the importance of collaborative work with like-minded countries. Priorities include building international resilience, supporting democracy and human rights, and the protection of research and intellectual property.
- In March 2021, the UK published its Integrated Review of Security, Defence, Development and Foreign Policy, which highlighted the importance of building alliances and strengthening bilateral ties with like-minded countries beyond the European Union. Canada is mentioned as a "force for good" partner.

Enhanced Strategic Coordination

Canada and the UK collaborate on national security issues in global fora, including through their membership in the Five Eyes alliance. This multilateral engagement, as well as wide-ranging activities at the bilateral level, could benefit from enhanced strategic coordination among high-level officials.

With evolving threats from state and non-state actors, Canada and the UK could explore options for a national security strategic dialogue. Potentially led by Canada's NSIA and the UK's NSA, this would allow for more frequent and formalized exchanges that would facilitate more effective responses to common threats.

Priority Topics

The following issues are proposed for further discussion with the UK:

- **Foreign Interference,** as enhanced collaboration would help prevent, identify, mitigate and respond to foreign interference domestically. Internationally, enhanced Canada-UK collaboration could bolster multilateral action against foreign interference practices from certain countries.
- **Economic Security,** with a specific focus on strengthening the research security culture of academic institutions and private sector organizations as well as protecting global supply chains (semiconductors, critical minerals, energy) to ensure safe and reliable procurement.

- **Societal Resilience and Trust,** to find solutions to prevent the erosion of public trust in national security that hampers the government's ability to establish relationships with various communities, and which can also affect the prevention of violent extremism.
- **Emerging Technology and Cyber Values,** to jointly develop frameworks to guide the use of these technologies to prevent illegal activities, while ensuring the protection of human rights, privacy and ethical considerations. Of particular interest: social media, artificial intelligence, encryption and quantum computing.

Possible Next Steps

In early January, the Interim Clerk of the Privy Council met with High Commissioner Goodale to discuss his recent letter. Possible next steps to suggest for continuing a potential Canada-UK strategic dialogue on national security include:

- A call between the Interim Clerk of the Privy Council and the UK Cabinet Secretary to formally establish the strategic dialogue.
- Regular discussions (twice yearly) between Canada's NSIA and the UK's NSA to provide overall direction to the strategic dialogue.
- Possible interaction between DMNS and its UK equivalent (National Security Council Officials – "NSCO") to discuss high-level NS policy questions of mutual concern.
- Regular meetings of DG-level working group to develop a roadmap and deliverables for the four key national security issues.

TAB C
Onglet C

Enhanced Canada-UK National Security Collaboration

Background

- On November 19, 2021, High Commissioner (HC) Ralph Goodale sent a message to national security Deputy Ministers to propose enhanced Canada-UK cooperation on national security issues.
- The interim Clerk of the Privy Council met with HC Goodale in January 2022 to discuss this initiative and potential next steps.
- On February 7, 2022, DMs from the national security community will discuss areas of focus for enhanced Canada-UK collaboration with HC Goodale.

Considerations

- Mandate letters highlighted the importance of collaborative work with like-minded countries. Priorities include building international resilience, supporting democracy and human rights, and the protection of research and intellectual property.
- In March 2021, the UK published its Integrated Review of Security, Defence, Development and Foreign Policy, which highlighted the importance of building alliances and strengthening bilateral ties with like-minded countries beyond the European Union. Canada is mentioned as a "force for good" partner.

Enhanced Strategic Coordination

Canada and the UK collaborate on national security issues in global fora, including through their membership in the Five Eyes alliance. This multilateral engagement, as well as wide-ranging activities at the bilateral level, could benefit from enhanced strategic coordination among high-level officials.

With evolving threats from state and non-state actors, Canada and the UK could explore options for a national security strategic dialogue. Potentially led by Canada's NSIA and the UK's NSA, this would allow for more frequent and formalized exchanges that would facilitate more effective responses to common threats.

Priority Topics

The following issues are proposed for further discussion with the UK:

- **Foreign Interference,** as enhanced collaboration would help prevent, identify, mitigate and respond to foreign interference domestically. Internationally, enhanced Canada-UK collaboration could bolster multilateral action against foreign interference practices from certain countries.
- **Economic Security,** with a specific focus on strengthening the research security culture of academic institutions and private sector organizations as well as protecting global supply chains (semiconductors, critical minerals, energy) to ensure safe and reliable procurement.

- **Societal Resilience and Trust,** to find solutions to prevent the erosion of public trust in national security that hampers the government's ability to establish relationships with various communities, and which can also affect the prevention of violent extremism.
- **Emerging Technology and Cyber Values,** to jointly develop frameworks to guide the use of these technologies to prevent illegal activities, while ensuring the protection of human rights, privacy and ethical considerations. Of particular interest: social media, artificial intelligence, encryption and quantum computing.

Possible Next Steps

In early January, the Interim Clerk of the Privy Council met with High Commissioner Goodale to discuss his recent letter. Possible next steps to suggest for continuing a potential Canada-UK strategic dialogue on national security include:

- A call between the Interim Clerk of the Privy Council and the UK Cabinet Secretary to formally establish the strategic dialogue.
- Regular discussions (twice yearly) between Canada's NSIA and the UK's NSA to provide overall direction to the strategic dialogue.
- Possible interaction between DMNS and its UK equivalent (National Security Council Officials – "NSCO") to discuss high-level NS policy questions of mutual concern.
- Regular meetings of DG-level working group to develop a roadmap and deliverables for the four key national security issues.

TAB D
Onglet

UNCLASSIFIED

Inventory of ongoing Canada-UK bilateral and multilateral engagement on national security issues

Area of Focus	Name	Scope/Mandate	Canada Lead & Intl Participants
Cyber Security/Operations	Ottawa 5	Discussion on cyber security policy issues including ransomware, supply chain security, emerging technology, advanced cyber threats, etc. Includes Trusted Markets Working Group	PS Five Eyes
Cyber Security/Operations	Five Eyes Digital Service Providers Working Group	Aims to share information, exchange views and work collaboratively to support effective policy development on the cyber security risks associated with Digital Services Providers.	PS/CSE Five Eyes
Cyber Security/Operations	G7 Virtual Network on Technical Standards	To operationalize the Leader level commitment from Carbis Bay, the G7 Virtual Network will: a. Help the G7 collectively take a more strategic and proactive response to shaping the future frontiers of the global economy by increasing coordination on regulations, technical standards and norms. b. Provide strategic advice that links the specific challenges to the development and adoption of technical standards to the big picture of G7 policy and geo-strategic objectives. Advice will focus on areas where there is a need for enhanced G7 coordination not already covered through existing mechanisms.	GAC G7
Cyber Security/Operations AND Military-Military Cooperation	European Centre of Excellence for Countering Hybrid threats	The European Centre of Excellence for Countering Hybrid Threats (a.k.a Hybrid CoE) is an international, independent network-based organization promoting a whole-of-government and whole-of-society approach to countering hybrid threats	PS/DND/CAF 29 member states (including UK and Canada as Steering Board members)
Cyber Security/Operations AND Military-Military Cooperation	Defence Cyber Contact Group	*Available at higher classification*	DND Five Eyes
Economic Security and Resilience	Foreign Investment Intelligence Review Exchange (FIIRE)	Collaboration and intelligence sharing on investment security issues.	CSIS (CSE also participates) Five Eyes

Economic Security and Resilience	Five Eyes Regulators of Foreign Investment (FERFI)	Group of lead regulators is working to identify key issues and address challenges facing the administration of our respective investment review regimes, in particular from a national security perspective. Runs alongside FIIRE.	ISED Five Eyes
Economic Security and Resilience	G7 Investment Screening Expert Group (ISEG)	ISED has been participating in ISEG under the G7 "Finance Track" with Finance Canada (overall lead). The G7 ISEG has been an important technical forum to share best practices, trends, and updates on investment screening.	Finance US, UK, Germany, Italy, Japan
Economic Security and Resilience	The National Technology and Industrial Base (NTIB) Investment Security Working Group	Comprised of people and organizations engaged in national security and dual-R&D, production, maintenance, and related activities. The NTIB, as established by 10 U.S.C. §2500, is intended to support national security objectives of the U.S., including supplying military operations; conducting advanced R&D and systems development to ensure technological superiority of the U.S. Armed Forces; securing reliable sources of critical materials; and developing industrial preparedness to support operations in wartime or during a national emergency. The Investment Security Working Group has focused on sharing best practices related to foreign investment review, such as methods for investment detection and assessment.	ISED (Investment WG lead) & DND (overall NTIB lead) US, AUS, UK
Economic Security and Resilience	Allied Economic Forum - Track 1.5 at Centre for Strategic International Studies	Track 1.5 series of conferences (typically three per year) organized by the Center for Strategic and International Studies (CSIS.org) in Washington, D.C. Topics discussed pertain to foreign investment review, export controls, science and research, and supply chains in the context of shared concerns related to national security and economic prosperity.	ISED & GAC 10 member states including U.S., Australia, EU members, Japan
Economic Security and Resilience	G7 Panel on Economic Resilience	Under the banner of its G7 presidency, the U.K. created the independent G7 Panel on Economic Resilience with a mandate to develop recommendations for G7 Leaders on a long-term approach to global economic resilience. One of the Panel's recommendations was that G7 countries intervene collectively, including with the business sector, to design resilient and open innovation-friendly market systems in critical sectors affecting national, economic or human security. It is unknown if Germany will continue this initiative during their G7 year.	GAC G7 (Panel of eight experts, one appointed by each G7 Leader)

Economic Security and Resiliency	Five Eyes Operations Committee	Committee of senior investment review practitioners focused on trends and issues emerging from case reviews.	ISED Five Eyes
Export Controls	Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Good and Technology (WA)	Forum to discuss technical and policy issues with regard to dual-use and military goods and technology. Participating States seek to ensure that transfers do not contribute to the development or enhancement of military capabilities which undermine these goals, and to ensure that these items are not diverted to support such capabilities. The WA is also intended to enhance cooperation to prevent the acquisition of armaments and sensitive dual-use items for military end-uses, if the situation in a region or the behaviour of a state is, or becomes, a cause for serious concern to the Participating States. Complements and reinforces, with minimal duplication, other export control regimes for weapons of mass destruction and their delivery systems.	GAC 42 states including Five Eyes, various EU and NATO members, Russia.
Hostile State Activity	Five Country Ministerial	2021 meeting included commitment to work within FCM and with likeminded partners through multilateral for a to share experiences and report on progress to build collective resilience in the academic and R&D sectors against foreign interference and unwanted knowledge transfer.	PS Five Eyes
Hostile State Activity	G7 Working Group on Security & Integrity in the Global Research Ecosystem	The WG will develop a common set of principles which, when implemented, will help to protect the research and innovation ecosystem across the G7 from risks to open and reciprocal research collaboration, and preserve the principles of open science and research freedom and independence. The Group will develop proposals for a virtual academy and toolkit, bringing together and developing the skills and experience of researchers, innovators, business leaders, and policy makers from any nation to develop a shared understanding of research integrity and security. This will embed the behaviours, systems and processes needed to protect valuable knowledge and technology assets where necessary, allowing international collaboration to continue with confidence.	ISED G7 (UK, Canada co-lead)
Military-Military Cooperation	Combined Space Operations Initiative (CSpO)	A group to enable and enhance cooperation on defence space activities through strengthening deterrence, improving resilience, optimizing resources, and advancing policy.	DND/CAF Five Eyes, France, Germany

Technology and Innovation	Emerging Technology Analytical Community	Analytical forum on strategic emerging technologies.	PCO (lead, CSIS, CSE, PS participate) Five Eyes
Technology and Innovation	Multilateral Action on Sensitive Technologies (MAST)	MAST is a group of countries instituted through the efforts of the U.S. State Department, but also includes U.S. Treasury/CFIUS colleagues in an effort to share information on regulatory processes related to sensitive technologies. Subjects have included export controls, research security and foreign investment review as tools to limit the transfer of sensitive technology causing national security concerns.	GAC (lead, with ISED leading on topics including foreign investment review; PS, participate) Five Eyes+, 15 countries total
Technology and Innovation	G7 Digital and Technology Track	The agenda is set by the G7 President each year. As part of its G7 Presidency this year, the U.K. is holding a Future Tech Forum on November 29-30 to create opportunities to learn about and influence the potential of the next generation of tech, to transform our societies and to identify the public policy questions that governments will need to consider over the next 5-10 years. It is unknown if Germany will continue this initiative during their G7 year.	ISED G7
Technology and Innovation	Global Partnership on Artificial Intelligence	Aims to bridge the gap between theory and practice on AI by supporting cutting-edge research and applied activities on AI-related priorities	ISED 25 members including Five Eyes, France, Germany, EU, Japan.
Technology and Innovation AND Military-Military Cooperation	AI Partnership for Defence (PfD) Initiative	Created by the US Joint Artificial Intelligence Centre (JAIC). created the AI Partnership for Defense (PfD). Serves as a recurring forum to discuss allied defence efforts in AI. The first three meetings were hosted by the US and focused on best practices for ethical principles, data, and human capital. The UK hosted the fourth PfD in October 2021 and the meeting focused on governance. Canada will host the fifth meeting virtually in early 2022, the topic has yet to be determined.	DND/CAF (lead) 16 member countries: US, UK, Canada, Australia, France, Japan, Finland, Sweden, Norway, Denmark, Estonia, Israel, Korea, Germany, the Netherlands and Singapore

E

A JOINT PUBLICATION OF
THE DANIEL K. INOUYE ASIA-PACIFIC CENTER FOR SECURITY STUDIES
AND THE MACDONALD-LAURIER INSTITUTE

5 EYES

Opportunities and Challenges in the New Strategic Landscape

John Hemmings
Peter Varnish

September 2021

The authors of this document have worked independently and are solely responsible for the views presented here. The opinions are not necessarily those of the Macdonald-Laurier Institute, its Directors or Supporters, or those of the Daniel K. Inouye Asia-Pacific Center for Security Studies and the United States Government.

Cover photo credit: Renée Depocas (using iStock)

Contents

Foreword 4

Executive Summary / Sommaire 6

Introduction 13

Technology 21

Information, Influence and Interference 31

Military 38

Economics 47

Conclusion 54

About the authors 57

Appendix: Interviews 58

References 62

Endnotes 78

Foreword

As Canada considers the global system, it sees much that is of concern to it. The rise of an authoritarian China under Xi Jinping and the restoration of Russian autocracy under Vladimir Putin are arguably the two most significant events affecting the current global system. Both men have secured power inside their own borders and are increasingly confident of their ability to project their norms and preferences externally.

Under their leadership, China and Russia are taking increasingly assertive actions to reshape the international system and constrain the liberal democratic West using a range of non-kinetic tools. While the threats from China and Russia are different in level and kind, they present a challenge that requires a collective response.

Over the past few years, there are signs that the Five Eyes may become a focal point of that response. Such a possibility is the subject of this timely and detailed paper, which attempts to deal with the important question of how the Five Eyes should – or should not – be used in response against these new authoritarian powers. It does so in a way that I think is very useful; it asks security experts across the five nations for their own opinions on how the Five Eyes might best be used to respond to the subversion and non-kinetic attacks of our foes.

The result is a list of highly detailed recommendations; I hope that Canada's political leadership will consider the merits of these recommendations in their deliberations.

Within the Five Eyes, there is still uncertainty if the group is the right one for responding to the unique challenges posed by China and Russia. Historically, it was used to fight fascism during the Second World War and then Soviet expansionism during the Cold War. It was remarkably successful at both endeavours and while some have criticized the group's intrusion into our own civic space, the liberal democracies have successfully limited and restrained abuses through legislative oversight.

The Five Eyes have been – for many decades – the guardians of our freedoms and it is worth remarking on how central that role has been since its founding. If we only consider the *Atlantic Charter* – the product of a historic wartime meeting between President Franklin Roosevelt and Prime Minister Winston Churchill in our own Placentia Bay, Newfoundland, we can see that the vision laid out in the Charter is one that still underpins the current global order.

At that time, the US and UK put forward the principle of non-territorial expansion. In an age when China now claims a sea larger than the Mediterranean while Russia annexes Crimea and invades Eastern Ukraine, this is significant. Both leaders had called for an order in which people's self-determination is respected. In an age in which both Russia and China attempt to rule peoples inside their historic imperial boundaries, this is significant.

I don't think the Five Eyes group should be the only response to the challenges posed by Russia and China – and, importantly, this paper does not make that assertion either. However, I believe the Five Eyes is an important part of the response, given the innate strengths of the group. This report makes a bold attempt to define that role and puts forward a number of concrete proposals in the spirit of democratic debate and discussion.

I have no doubt that Five Eyes governments will look at the recommendations differently and with varying degrees of engagement. Nevertheless, I hope they will encourage discussion and, ultimately, appropriate action.

Richard Fadden *is former national security advisor to the Prime Minister of Canada and former director of the Canadian Security Intelligence Service.*

Executive Summary

State competition is changing, in a shift towards deniable, intrusive, and non-military threats against all sectors of society – technology, information, democratic institutions, and trade. As a result, liberal democracies are increasingly on the back foot and looking for collective ways to respond and deter.

Among the most important collective approaches is the Five Eyes, a historical group that includes the United States, the United Kingdom, Australia, Canada, and New Zealand. Though it has long been associated with intelligence-sharing, the group has become increasingly visible as it issued a five-country statement on China's repression in Hong Kong in November 2020 and most recently, as New Zealand publicly questioned an expansion of the group's diplomatic function. It is clear the group is evolving to meet today's challenges, but it is not yet clear as to its ultimate direction. In some ways, this paper is intended to encourage a discussion to help security practitioners and policy-makers from all five countries understand their choices.

Historically, the primary strength of the Five Eyes partnership has been organizational. The partnership has developed a process that enables the five countries to pool resources for their common security at a deeply institutionalized level. Their cooperation, which began with the *Atlantic Charter* and UKUSA Agreement, has its foundation in signals intelligence-sharing (i.e., sharing foreign intelligence gathered from communications and information systems). The relationship developed into cooperation across a wide swath of areas, including human intelligence-sharing (i.e., information gleaned from personal contacts), technological co-development, and military equipment and communications interoperability.

Today's authoritarian powers, the People's Republic of China (PRC) and Russia, understand the importance of data-oriented information and technologies (AI, 5G, and Big Data Analytics) and are pursuing aggressive strategies to surpass the West in numerous dual-use (military and civilian) sectors. In China, Xi Jinping has called for the Party to "keenly grasp the historic opportunity that informatization has offered" and is undertaking a major digital in-

frastructure campaign meant to help China surpass the United States in these technologies and to promote the "Chinese model" overseas.

The development of technologies that enable the transfer, collection, and harvesting of data is having a sizeable impact on the information environment, affecting political narratives, political will, and state legitimacy, in what amounts to an updated version of the political warfare threat posed by the Soviet Union during the Cold War.

Unlike the Cold War period, however, China and Russia are challenging global governance, maritime law, and international diplomacy. China's growing economic heft in particular, along with its command-and-control economy, give it increasing leverage over the international trading system. Meanwhile, by using its economic weight and access to its market to punish and isolate individual Five Eyes members, it is also threatening the long-term cohesion and coherence of the alliance. Therefore, as we argue in this paper, the Five must develop the capability for analysing and countering China and Russia's interference and propaganda, and develop practical non-military ways to deter them.

We carried out extensive interviews of defence and security practitioners across the Five asking what ways the Five Eyes might deal with today's challenges: a comprehensive list of the people interviewed is included in the appendix. The following list of recommendations are the result of those discussions:

- Create a Five Eyes tech centre that could take promising technologies from the private sector, from the technology cooperation program (TTCP), and from academia, and provide a venue for collaborative projects using specific technologies.
- Study whether the National Technology Industrial Base (NTIB) would be a suitable venue for initiating closer Five Eyes technological development over the long-term.
- Create interagency public/private working groups to coordinate on technology standards. The Five need to align more closely on Internet protocols and with the Third Generation Partnership Project, the International Telecommunication Union, and the International Organization for Standardization.
- Create a fusion centre to undertake classified analysis and operations on information operations/interference as well as a semi-public "excellence centre" to help disseminate the output of the fusion centre among more peripheral partners of the Five, including Japan, France, South Korea, Germany, etc.
- Create a counter-interference handbook that analyses Russian and Chinese interference both inside the West and in other countries. Use the handbook to offer lessons learned, instruct on counter-measures, and outline policies.

- Create a Five Eyes Defence Policy Bureau to generate ideas upon which the group can act in geostrategic areas of importance, such as the South China Sea and the Arctic.
- Develop robust defence guarantees among the Five Eyes partners so each supports the others when operating together in contested waters to back up the mutual defence commitments from NATO (North Atlantic Treaty Organization) and ANZUS (Australia, New Zealand, and United States).
- Increase political and security consultations among the Five to address the economic warfare intended to degrade any member's sovereignty or isolate members of the group from each other.
- Carry out supply chain security audits across the defence and dual-use sectors of national economies. Agree upon a policy to immediately diversify away from over-reliance on PRC suppliers in strategic sectors.
- Develop a collective approach towards economic warfare and a range of proportionate economic counter-measures that everyone in the group will use.
- Institute regular meetings between heads of Five Eyes investment screening bodies: the heads of the Committee on Foreign Investment in the United States (CFIUS), Australia's Foreign Investment Review Board (FIRB), the Department of Innovation, Science and Economic Development Canada (ISEDC), the Investment Security Unit (UK) and New Zealand Treasury unit should meet regularly to exchange notes on nefarious investors, lessons learned, and best practices.
- Carry out a feasibility study on free trade agreements, bilateral or multilateral, and consider combining them into one agreement.

Our hope is that this paper's recommendations will foster evolution – not revolution – within the Five Eyes grouping. This might include discussions leading to the solutions for urgent and immediate threats (collect the low-hanging fruit) and will also open up for discussion and debate long-term structural changes within the security and defence communities of our Five nations.

Sommaire

La concurrence entre États change, évoluant indéniablement vers une forme intrusive de menace non militaire contre tous les secteurs de la société – technologies, informations, institutions démocratiques et commerce. C'est pourquoi les démocraties libérales se retrouvent de plus en plus en position désavantageuse et cherchent collectivement des outils de riposte et de dissuasion.

Au cœur des approches collectives les plus importantes, on retrouve le « Groupe des cinq » [ou *Five Eyes*], une alliance emblématique qui réunit les États-Unis, le Royaume-Uni, l'Australie, le Canada et la Nouvelle-Zélande. Bien que le *Five Eyes* soit depuis longtemps associé au partage de renseignements, il a amélioré sa visibilité de façon croissante dès la publication en novembre 2020 de la déclaration commune de ses membres sur la répression de la Chine à Hong Kong et encore, plus récemment, lorsque la Nouvelle-Zélande a publiquement questionné l'élargissement de sa fonction diplomatique. De toute évidence, le Groupe évolue pour relever les défis actuels, mais son orientation définitive n'est pas encore claire. D'une certaine manière, le présent document vise à favoriser une discussion pour aider les praticiens du domaine de la sécurité et les décideurs politiques des cinq pays membres à comprendre quels sont leurs choix.

Historiquement, la principale force de l'alliance *Five Eyes* a été d'ordre organisationnel. L'alliance a mis sur pied un processus qui permet aux cinq pays membres de mettre en commun leurs ressources en vue d'assurer leur sécurité commune au moyen d'un processus d'institutionnalisation poussée. La collaboration, qui a débuté avec la signature de la *Charte de l'Atlantique* et du traité UKUSA, repose sur le partage de renseignements électroniques (c'est-à-dire le partage de renseignements étrangers recueillis à partir de systèmes de communication et d'information). Cette relation s'est transformée en coopération dans un large éventail de domaines, notamment le partage de renseignements humains (c'est-à-dire les informations recueillies à partir de contacts personnels), le codéveloppement technologique et l'interopérabilité des équipements et des communications militaires.

Les puissances autoritaires actuelles – la République populaire de Chine et la Russie – comprennent l'importance de l'information et des technologies axées sur les données (IA, 5G et analyse des mégadonnées) et mettent en œuvre des stratégies agressives visant à devancer l'Occident dans de nombreux secteurs à double usage (militaire et civil). En Chine, Xi Jinping a appelé le Parti à « saisir vivement l'occasion historique qu'offre l'informatisation », tout en lançant une grande campagne d'infrastructure numérique destinée à aider la Chine à prendre le pas sur les États-Unis dans ces technologies et à promouvoir le « modèle chinois » à l'étranger.

Le développement de technologies permettant le transfert, la collecte et la récolte de données a un impact considérable sur l'environnement de l'information, ce qui influe sur le discours politique, la volonté politique et la légitimité de l'État, dans le cadre de ce qui est en fait une version actualisée de la menace de guerre politique posée par l'Union soviétique pendant la guerre froide.

Contrairement à la période de la guerre froide, cependant, la Chine et la Russie remettent en question la gouvernance mondiale, le droit maritime et la diplomatie internationale. Le poids économique croissant de la Chine en particulier, conjugué à la nature planifiée de son économie, favorise l'influence de ce pays sur le système commercial international. Parallèlement, en utilisant son poids économique et l'accès à son marché pour pénaliser et isoler des membres individuels du *Five Eyes*, la Chine menace également la cohésion et la cohérence à long terme de l'alliance. Par conséquent, comme nous le soutenons dans ce document, le *Five Eyes* doit développer la capacité d'analyser et de combattre l'ingérence et la propagande de la Chine et de la Russie et adopter des méthodes concrètes de dissuasion non militaires contre ces pays.

Nous avons mené des entretiens approfondis avec des praticiens de la défense et de la sécurité des cinq pays membres du Groupe et leur avons demandé comment le *Five Eyes* pourrait faire face aux défis actuels : la liste complète de ces personnes figure en annexe. Les recommandations que voici ont été préparées à partir de ces entretiens :

- Créer un centre technologique « *Five Eyes* » en vue de mettre au point des technologies prometteuses issues du secteur privé, du programme de coopération technologique (TTCP) et du monde universitaire, et offrir un endroit pouvant accueillir des projets de collaboration appuyés sur des technologies précises.
- Étudier si le concept de base industrielle technologique nationale (NTIB) permettrait d'amorcer un développement technologique *Five Eyes* plus étroit à long terme.
- Mettre sur pied des groupes de travail publics et privés interagences pour coordonner les normes technologiques. Les cinq pays

membres du Groupe doivent s'aligner plus étroitement sur les protocoles Internet et le Projet de partenariat de troisième génération, l'Union internationale des télécommunications et l'Organisation internationale de normalisation.

- Créer un centre intégré qui entreprendrait des analyses et des opérations secrètes sur les activités d'information ou l'ingérence, ainsi qu'un « centre d'excellence » semi-public pour aider à diffuser les produits du centre intégré parmi les partenaires à la périphérie des cinq pays membres du Groupe, notamment le Japon, la France, la Corée du Sud, l'Allemagne, et ainsi de suite.
- Concevoir un manuel en matière de contre-ingérence qui analyse l'ingérence russe et chinoise tant en Occident que dans d'autres pays. Présenter les leçons apprises, les contre-mesures et les grandes lignes des politiques sur la base de ce manuel.
- Créer un bureau de la politique de défense du *Five Eyes* pour générer des idées pouvant servir de fondement aux actions du Groupe dans les zones géostratégiques importantes, notamment la mer de Chine méridionale et l'Arctique.
- Mettre en place des garanties de défense solides permettant aux partenaires du *Five Eyes* de se soutenir mutuellement lorsqu'ils opèrent ensemble dans des eaux litigieuses, en appui des engagements de défense mutuelle de l'OTAN (Organisation du traité de l'Atlantique Nord) et du réseau ANZUS (Australie, Nouvelle-Zélande et États-Unis).
- Accroître les consultations sur la politique et la sécurité au sein des cinq pays membres du Groupe pour se défendre contre la guerre économique visant à compromettre la souveraineté d'un membre ou à isoler les membres les uns des autres.
- Procéder à des vérifications de la sécurité de la chaîne d'approvisionnement liée à la défense et aux secteurs à double usage des économies nationales. Convenir d'une politique de diversification immédiate pour éviter une dépendance excessive à l'égard des fournisseurs chinois dans les secteurs stratégiques.
- Développer une approche collective de la guerre économique et créer une gamme de contre-mesures économiques proportionnées que tous les pays membres du Groupe utiliseront.
- Organiser des réunions régulières entre les responsables des organismes de contrôle des investissements du *Five Eyes* : les responsables du Comité des investissements étrangers aux États-Unis (CFIUS), du *Foreign Investment Review Board* (FIRB) de l'Australie, du ministère de l'Innovation, des Sciences et du Développement économique du Canada (ISDE), de l'*Investment Security Unit* (Royaume-Uni) et des autorités du Trésor néo-zélandaises devraient se rencontrer régulièrement pour échanger des informa-

tions sur les investisseurs malveillants, les enseignements tirés et les meilleures pratiques.

- Réaliser une étude de faisabilité sur les accords de libre-échange, bilatéraux ou multilatéraux, et envisager de les combiner en un seul accord.

Nous espérons que les recommandations présentées dans ce document favoriseront l'évolution – il n'est pas question ici d'une révolution – au sein du ***Five Eyes***. Elles pourraient comprendre des discussions pour trouver des solutions aux menaces urgentes et immédiates (cueillir les fruits à portée de main), mais aussi permettre de débattre des changements structurels à long terme au sein des milieux de la sécurité et de la défense de nos cinq nations.

Introduction

"The role of non-military means of achieving political and strategic goals has grown and in many cases, they have exceeded the power of force of weapons in their effectiveness. All of this supplemented by military means of a concealed nature."

– General Valery Gerasimov,
Russian Chief of the General Staff (McKew 2017)

The Changing Security Environment

Over recent years, the international security situation has worsened and become increasingly fluid and dynamic, marked by hybrid warfare, grey-zone tactics, and non-kinetic threats; this entails political warfare, economic warfare, cyber operations, and strategic messaging against a target state without the use of conventional military means. In addition to the continuing threat from non-state actors such as violent extremists, the group known as the Five Eyes, which includes the United States, the United Kingdom, Australia, Canada, and New Zealand, face a number of intensifying and persistent threats from state actors, such as Russia, China, and Iran, operating alone or, occasionally, together.

The 2018 *US National Defense Strategy* points to "increased global disorder, characterized by decline in the rules-based international order" (United States 2018), while the UK's *Integrated Review of Security Defence, Development and Foreign Policy* cites the "systemic competition, including between states, and between democratic and authoritarian values and systems of government" (United Kingdom 2021). Canada's 2017 defence policy, *Strong, Secure, Engaged*, notes that some of the drivers of this new insecure age include "the shifting balance of power, the changing nature of conflict, and the rapid evolution of technology" (Canada 2017).

This shifting balance of power has been focused, to some extent, on the post-

Cold War economic changes that have narrowed the power gap between a rising China and the United States, the latter of which remains the lead western power.[1] This dynamic stems from broader system-wide changes to the balance of power between the Western liberal democracies, who emerged victorious from the Cold War, and their former adversaries.

In the years leading up to and following the end of the Cold War, Russia and China were disoriented and perplexed by the apparent failure of their centrally-planned economies and the seeming rejection of communism by their own populations. In regrouping, both determined to consolidate their domestic affairs. By 2012 they had strong leaders around whom state power has been centralized. As both states undertook internal consolidation through state-led campaigns to promote nationalism,[2] their foreign policies became increasingly assertive externally, and so both countries have begun to challenge the fundamental assumptions implicit in the rules-based order that we have inherited from the post-Cold War era.

By contrast, Western nations and their societies embraced the so-called "peace dividend" (Mintz 1995), moving toward neoliberal economic policies and an increased faith in multilateral institutions as a means of resolving conflict. During this period, the Western states went from viewing the Soviet Union and People's Republic of China as threats to be managed to attempting to bring them into the rules and norms of the global order. The hope was that they, too, would have a stake in the post-Cold War world. According to this line of thought, by including them in the World Trade Organization (WTO) and – in the case of Russia – giving them access to the World Bank and membership in the G7, Russia and China would plainly see the benefits of being "responsible stakeholders" (Zoellick 2005).

Since 2014, however, it has become clear that neither are fully content with the fundamental rules and norms established since the end of the Second World War. Russia has carried out two biological attacks on UK soil (McTague 2019), annexed Crimea (Hille et al. 2014), placed 100,000 troops along the Ukraine border, commenced militarization of the Arctic Sea, and launched a serious campaign of political warfare against Western democracies (Lewis 2020). China, for its part, has not only laid claim to a large portion of the South China Sea (backed by military bases on its newly-built islands (Phillips 2015)), but also it has begun a determined and vigorous effort to become a technological leader in a range of sectors in ways that threaten Western interests (Hemmings 2020). Like Russia, Beijing has begun a serious campaign of interference inside Western states, and its global ambitions can be seen with the increasing export of its authoritarian preferences in international standards (Ruhlig 2020), technology (Xi 2016), media (Xi 2013), and governance (Economy 2019).

The Nature of the Challenge

Both Russia and China are waging increasingly aggressive campaigns of political warfare (also known as "below-threshold conflict") designed to undermine the social, economic, and political resilience of the Five. China has also deployed cyber tools (aka cyber-warfare) in ways that have increased in scale and impact on democratic and social institutions (Greenberg 2018). While some of these tactics are reminiscent of Soviet "active measures" used against Western societies during the Cold War (United States 1986), today's political warfare has increased in intensity and deniability due to the proliferation of new information communications technologies and social media.

This report analyses today's state competition across the following sectors: **1) Technology:** how China and Russia are competing for dominance in a number of dual-use, data and information communications technologies; **2) Information, Influence and Interference:** how China and Russia have begun a significant campaign of interference and influence operations,[3] combined with an increased "discourse war" against the West in general, and liberal democracy in particular; **3) Military:** how China and Russia are using hybrid warfare and grey-zone tactics, including the threat of force, to effect territorial changes on land and on sea; and finally **4) Economics:** how both countries, but particularly China, have begun to hone their use of economic statecraft – using both economic carrots and sticks – against the Five and the companies in each nation in order to exert coercive leverage over their policy elites.

Perhaps what has been most challenging about this new era of competition is the fact that so much takes place in the grey zone and across deniable forums, such as the Internet. By using what can be termed "below-the-threshold-of-military means," these micro-attacks fall below Article V of the North Atlantic Treaty Organization (NATO)[4] and as such do not justify an armed response. However, when added together, the sum total of Russia's and China's cyber operations, information campaigns, mass theft of intellectual property in advanced technologies, and other acts, both covert and overtly hostile, still add up to a "significant" attack on the social and political resilience of the Five,[5] and as such require a coherent response.

Furthermore, China has begun to use its growing economic leverage to affect many of its bilateral relationships – including using market access, trade and investment – in ways that can only serve to coerce states into submitting to its policy preferences. As Eric Sayers, an Adjunct Senior Fellow from the Center for a New American Security (CNAS) states, "If a government or administration chooses to prioritize stability in their bilateral relationship with China above all else, it will prove next to impossible to counter gray zone activities. Beijing is expecting that no government will compromise a positive relationship with them over the micro-costs of gray zone activity."[6]

This might be seen in the example of Australia, one Five Eyes partner. Since around 2017, Australian policy experts noted a high level of political interference inside domestic politics, including (but not limited to) significant funding to both political parties (Uhlmann 2018), alleged elite-capture of political figures,[7] and increased influence over its Chinese-language media, academia, and think tanks (Ross 2020). After Prime Minister Malcolm Turnbull oversaw the passage of a foreign interference law in 2018 (Turnbull 2017), Beijing paused high-level visits, lashed out at Australia in its state media, and froze ministerial exchanges. While Australia made it clear that the new law was not directed at any one country, the Chinese response was one of sustained political and economic pressure.

In July 2020, the *Global Times* newspaper tweeted, "If Australia provokes China more, China will fight to the end to defend its core interests. Australian education, mining, and agriculture all desire improved ties with China" (Global Times 2020). In November 2020, the Chinese Embassy in Canberra leaked a list of 14 areas where it implied that Australia should change its behaviour if it wanted relations to improve (Galloway 2020). One such change included restricting criticism of China by Australian think tanks, an authoritarian preference that would be impossible for liberal democracies to implement without fundamentally reshaping free speech norms.

By contrast, China's influence operations have had a "Stockholm Syndrome" effect (Anderlini 2021), either fragmenting the resolve of Western governments and political elites, or seemingly influencing them to adopt positions similar to Beijing's. For example, Canada's Ambassador to China was removed in 2019 after he made remarks that seemed overly supportive of the Chinese regime (Reuters 2019). Meanwhile, the former UK Chancellor referred to the deployment of the HMS Queen Elizabeth to the Pacific as "gunboat diplomacy of a quite old fashioned kind" (BBC 2019). New Zealand has balanced its own criticism of China with recommending that Australia show China more "respect" (Dziedzic 2021).

Enter the Five

While Western states have begun to respond to this new political warfare, their response remains disparate, deliberately confused by the oblique and piecemeal tactics that China and Russia have adopted with their combined use of coercive economic statecraft and their influence among policy elites. This paper was prompted by a growing sense within the Five that the Five Eyes grouping has a number of characteristics that make it well suited for dealing with this new information age, one in which data technologies will play a crucial role in competition.

As is already well-known, the Five Eyes group was established by the US and UK (United Kingdom 2010) as an intelligence-sharing and technology col-

laboration arrangement, which was later extended to Canada, Australia, and New Zealand so that they could pool resources and cryptographic discoveries in the war against the Axis powers. Cooperation increased during the Cold War as the Five added human intelligence, military equipment interoperability, and defence research and development (R&D) agreements to the growing relationship.

While it is often called the Five Eyes alliance, technically speaking it is not really an alliance at all, since it lacks an *explicit* defence guarantee, which is an essential ingredient in most definitions of alliances in the broader literature (Wilkins 2012, 55). One might argue that it has an implicit defence guarantee[8] since the Five are bound together by two other treaty alliances, NATO and ANZUS (Australia, New Zealand, and United States).[9] However, the group itself lacks an explicit mutual defence clause, a secretariat, or a single founding treaty;[10] nor does it have a coordinating body to deal with the broad array of security cooperation that occurs in its name.

While it is often called the Five Eyes alliance, technically speaking it is not really an alliance at all.

Instead, the Five is an organizing principle, or what one interviewee called a "forum shop," a "process,"[11] that seems to develop new functions in response to needs. According to one interviewee,[12] there are many hundreds of agreements between the Five on a range of topics that prescribe the various ways in which they will cooperate. Many of these have been extremely effective at creating personal relationships that have, over many years, proven to be essential in getting things done expeditiously and without hindrance in both peacetime and war.

The truth of this becomes clear in looking at its organization structure – or lack of one. The Five Eyes arrangement has developed into an intricate web of discreet groupings that cover an intimate but wide-ranging number of sectors.[13] There are working-level groups and meetings across diverse groups of departments that cover everything from defence research to passports and borders, maritime domain awareness, law enforcement, intelligence oversight, and immigration. Even the Attorneys General from each country have a "Quintet" group (Public Safety Canada 2019).

Most recently, the five foreign ministers have begun to meet, issuing joint statements on, for example, the nature of Hong Kong's Legislative Council elections. Much of the work in the Five takes place at the working level, rather than the political level, with the latter only beginning to occur more often in recent years. The development of the foreign ministers' group represents a renewal of the top-down approach – political rather than bureaucratic leadership – indicating a growing appreciation of the network necessary to meet today's challenges.

Still, the Five continues to be marked by its ad hoc, fluid informality. As one interviewee states, the historic conditions by which the US, UK, Canada, Australia, and New Zealand came together were unique, and not simply in the sense that they were allied in the Second World War: "They all emerged from the same cultural, linguistic, and ideological grouping. Broadly speaking, they share a common legal system, a common history, and similar democratic traditions, and this has been the glue that kept them together, a glue that has been unseen and unstated" (Eyal 2020). The same is true in practical terms, as the Five share a common approach towards personnel security clearance as well as a common classification system, allowing for regular and institutionalized sharing of classified materials. In many ways, these processes constitute a "Five Eyes standard" to which other potential partners and allies – such as Japan – might aspire.

The Five have also developed a heightened level of military uniformity and cross-departmental personnel exchange programs – a set of "special relationships" – that ensure that different national departments are comfortable with each other and can work together well, in both the uniformed and civilian bureaucracies. In addition, there are multiple agreements within the group that help ensure that communications and military equipment is interoperable to foster greater operational cohesion.

While the Russians and Chinese pose many challenges below the level where they would trigger an armed response, they still affect the Five Eyes nations' national security. That said, the Five are in fact well-suited to address these challenges by virtue of their strengths and capabilities in the technology, information, military, and economic spheres. Some challenges, such as Chinese and Russian political warfare against the West, only require the restitution and updating of capabilities honed during the Cold War-era (Schoen and Lamb 2012), while others, such maintaining technological dominance, could be managed via enhancements to programs currently in place among the Five, such as complementary national industrial strategies and closer defence industrial collaboration.

While there is already some measure of Five Eyes scientific R&D in bodies like the Technical Cooperation Program (TTCP), there is relatively little co-development of the new dual-use technologies that will empower tomor-

row's warfighters. The recent addition of the United Kingdom and Australia to the National Technology and Industrial Base (NTIB) – a legal framework previously limited to the US and Canada – suggests that there are new avenues for expanding and opening up opportunities for innovation and collaboration, perhaps on a scale not seen since the Second World War (Kliman and Thomas-Noone 2018). While the possibilities are exciting, changes in the defence industry sector must be done carefully with each Five balancing its own national security and economic interests.

As this paper lays out, the Five might choose to work more closely together on a wider range of issues in the future, but the group would have to do so with care and forethought. The group needs to ensure that those responsible for defence and foreign policy in each of the Five can stand up for their own interests as the group collectively debates and determines a careful and steady evolution in approach toward our present challenges. They might even consider coordinating the Five at the national security council level since foreign policy, defence, and intelligence are all represented there. At present, there is a danger that multiple agencies and departments might seek to expand their Five Eyes remit without coordinating with each other, risking duplication and needless bureaucratic infighting.

The Five might choose to work more closely together on a wider range of issues in the future.

There should also be a "cut out" for the intelligence services since the nature of their cooperation is of a vastly different nature to those of defence and diplomacy. The intelligence services must be allowed to keep their activities as a "closed shop," though this might not be necessary in other sectors. So, while intelligence inter-agency cooperation should remain separate and distinct – perhaps even maintaining a monopoly on the term "Five Eyes," for example – there are nevertheless significant opportunities for expanding cooperation to other jurisdictions across a range of less sensitive areas. As just one example, current work in science and technology could expand to include other like-minded countries with advanced technologies, such as Japan, Taiwan, the Netherlands, Norway, or South Korea, but on a project-by-project basis. This would allow the Five to remain an intelligence group even while evolving into an organizing principle with various political, diplomatic, technological, and military streams of cooperation.

Methodology and Layout

This paper relies on open-source, unclassified materials, publicly available government documents, and interviews with experts. Given that any sort of expansion of the Five Eyes grouping – no matter how ad hoc – presents different political costs and benefits to each of the Five, this paper has sought to interview national security experts across all five countries and includes an appendix of those interviewed. The Five Eyes is a collective effort and so any study of the grouping that carries recommendations should reflect that. Most interviews were on the record and have been cited as such, but some remain anonymous according to the wishes of the interviewees.

These interviews were carried out by telephone or electronically between July and November 2020. We originally expected that this paper's analysis would follow the traditional DIME model (diplomatic, information, military, and economic), but after some consideration, we felt that the growing role of technology meant that it deserved its own chapter. As a result, this report will follow a TIME format (technology, information, military, and economic). This is not meant to imply that diplomacy is unimportant. Instead, each section's recommendations will seek to incorporate diplomatic features.

The first section will look at the challenges and opportunities the Five face in technology, with reference to R&D, investment, and standard-setting. The second section will look at the information and interference campaign taking place against the Five and try to determine a collective response. The third section will look at the military aspects of defence: how the Five might work with other like-minded groups such as the Quadrilateral Security Dialogue (or the Quad)[14] in the Indo-Pacific or NATO in Europe. Finally, the fourth section will cover the economic challenges and look at the difficulties the group faces in crafting responses to a new type of economic coercion and warfare. Given that China remains a major trading partner, a growing economic power, a growing source of advanced technologies, and a major source of investment for all five countries, this issue is complex and clearly requires much consideration.

Technology

"Disruptive technologies are constantly emerging, continually reshaping the world's competitive landscape, changing the balance of power among states."

– Outline of the National Innovation-Driven Development Strategy
(Central Committee of the Communist Party of China and the PRC State Council 2016a)

Technology collaboration – particularly that relating to code-breaking and cryptography – is central to the Five Eyes intelligence agreement and has been since the success of the allied war effort and victory over the Axis powers during the Second World War. The Manhattan Project was a part of this collaboration and it enabled the US and UK to become nuclear powers. Technology was also at the forefront of the West's decades-long battle against the Soviet Union and the Eastern Bloc and enabled our militaries to be increasingly competitive and interoperable. The United States – the West's primary military democracy – has enjoyed technological superiority ever since, allowing it to fight asymmetrically against less advanced foes such as Iraq's military, the Taliban, and ISIS in Iraq.

Three important trends are affecting today's strategic technologies. First, since the 1990s, information or data-led technologies – themselves the result of Western innovation – have been "bleeding" into the military space, changing how war is fought by disaggregating the "kill chain" (consisting of three actions: sensing, deciding, acting). The kill chain has moved from a predominantly single-platform approach to a highly-networked multi-platform approach that uses various sensors, satellites, command centres and, finally, highly intelligent or autonomous platforms that deliver kinetic effect to a target (Brose 2020).

Second, the most innovative and cutting-edge sources of these new "enabling technologies" (Horowitz 2018, 41) have been the civilian sector, not the defence sector.[15] That these predominantly civilian tech companies have in effect become dual-use has meant that there is a gap in mindset in companies like Google that are reluctant to work closely with the military. Conversely, many traditional defence industrial firms have tiny R&D budgets in sectors like artificial intelligence and quantum computing, so there is a risk that traditional militaries are being left behind in the innovation race. However, a third trend has seen the PRC and Russia adapt to this in their home markets, creating links between their civilian tech sectors and their militaries – a good example can be seen with China's Civilian-Military Fusion Doctrine. They have also significantly prioritized restructuring, joint operations (across services), hybrid warfare, advanced jamming techniques, precision strike capabilities, and increased R&D in those areas. According to many of our interviewees, Russia and the PRC have identified US and NATO core strengths and weaknesses, and have designed platforms and strategies to undermine those strengths and take advantage of the weaknesses.

The assumption that the West leads in military and civilian/military technology can no longer be taken for granted (Rogers 2020). The 2018 National Defense Strategy Commission's report to Congress made the following judgment: "America's military superiority… has eroded to a dangerous degree… It might struggle to win, or perhaps lose, a war against China or Russia" (Edelman and Roughhead 2018). In referring to the critical dependence of US battle systems on the electromagnetic spectrum (EMS) and Russian and Chinese efforts to challenge US superiority in that domain, the US Department of Defence (DOD) report, *Electromagnetic Spectrum Superiority Strategy*, asserts that "Our adversaries have recognized DOD's reliance on EMS-dependent capabilities and are seeking to exploit this vulnerability. They seek to restrict US spectrum access through international forums while they organize, train, and equip their forces for EMS advantage" (United States 2020a). There is growing concern within the Five that Russia and China present increasingly sophisticated and proven technological challenges to Western battle networks and civilian infrastructure.

Considering Russia

This challenge to Western technological dominance and the rise of Russian and Chinese military technological capability is a story of their actions and Western inaction. As UK Defence Minister Ben Wallace recently stated, "our enemies have studied our vulnerabilities and adapted far more quickly than us" (Warrell 2020). Russia, a relatively declining power, has focused its investments in two directions: select conventional military capabilities where it believes it holds comparative advantages over the West and "AI-driven military technologies" (Horowitz et al. 2018, 15-17).

Russia's approach has resulted in a major surge in their development of unmanned land, air, and sea-based systems, such as the *Nerebta*, the Uran-9, and the Orlan-10. In 2014, the Russian military approved a program called "The Creation of Prospective Military Robotics through 2025" and in 2016 it launched an annual conference called "Robotization of the Armed Forces of the Russian Federation" (Bendett 2017a). The goal of this annual event is to develop "unified interdepartmental approaches for the creation and development of military and special-purpose robotic complexes (RTCs)" (Bendett 2017b). Russian forces have also used drones and precision strikes in close conjunction with electronic warfare in both Syria and Ukraine, showcasing their challenge to US dominance in the electromagnetic spectrum (Keller 2019).

The latest State Armament Plan – GPV 2027 – focuses on improving Russia's ground forces, improving its rapid reaction and elite forces, strengthening its mobility, and updating its command-and-control system. Its technological focus is on long-range and precision strike weapons, including sea- and air-launched hypersonic and cruise missiles, including the nuclear-powered cruise missile, the 9M730 *Burevestnik*, which is said to be able to loiter indefinitely, or remain around a potential target until needed (Lendon 2018). Russian air defence systems – the S-400 and next generation S-500 – are considered among the world's best (Bowen 2020).

In addition, Russia has developed a hypersonic glide vehicle, an unmanned underwater vehicle with a nuclear payload (Gady 2016), and mission-specific deep-water submarines and space-based anti-satellite weapons (The Economist 2020). Also disconcerting is the progress of Russian planning and organization, shown in its ability to hold snap exercises fielding many hundreds of thousands of personnel. Between February and March 2014, during a time of heightened tensions with the West, Russia held a snap exercise with 150,000 personnel. In 2015, it held a snap exercise in the high north with 50,000 personnel. The 2018 annual military exercise *Vostok* was held with 300,000 soldiers, 1000 aircraft, and 80 warships and auxiliaries (Johnson 2018), an impressive feat if the numbers are to be believed. In early 2021 over 100,000 Russian troops were stationed on Ukraine's eastern border.

Considering China

The technology competition becomes even sharper when considering China, which has stated its intent to become the world's innovation leader, a "cyber superpower" using the umbrella strategy *Digital China* (Dorman and Hemmings 2021). Beijing has set about creating a range of strategies[16] and individual policies to enable it to lead in key technologies, such as 5G telecommunications, biotechnology, artificial intelligence, robotics, aerospace, nuclear power, microelectronics, quantum technologies, and space technology. In requiring that "Chinese communist party committees" be inserted into its private technology firms – the highest proportion of any business sector

(Cave et al. 2019) – and requiring that they collaborate with the military under the Civilian-Military Fusion Doctrine, China is addressing the gap between its state-owned defence industry and the advanced technology firms.

Beijing has also been highly adept at legally and illegally acquiring dual-use technology from the West in what FBI Director Christopher Wray has called "one of the largest transfers of wealth in human history" (Mead and Wray 2020). In 2017, the Intellectual Property (IP) Commission estimated that the US was losing nearly US$400 billion a year (Commission on the Theft of American Intellectual Property 2017) in IP theft, much of it to China. In addition to cyber-attacks, some of this IP theft has taken place in plain sight; People's Liberation Army (PLA) researchers have undertaken research in STEM (science, technology, engineering, and mathematics) programs within the universities of the Five (Joske 2018) and through the poorly-understood "Thousand Talents" program (Joske 2020), whereby China recruits international experts in science, innovation, and entrepreneurship.

Beijing has also been highly adept at legally and illegally acquiring dual-use technology from the West.

China has also used WTO non-compliant measures – such as forced joint ventures for foreign companies wishing to operate in China – to effect technology transfers in these dual-use sectors. It has also heavily subsidized strategic technologies such as information communications technologies, autonomous vehicles, and alternative energies in ways that have affected Western competitors. Huawei's gains in the European telecom market – it went from 2.5 to 25 percent market share between 2006 and 2014 (Le Corre and Sepulchre 2016, 113) – were aided by the US$100 billion in credit made available to the company through Chinese state-owned banks (Nakashima 2019).

China was predicted to spend US$563 billion on R&D in 2020, slightly less than the US outlay of US$609 billion. However, Beijing has raised its R&D spending by 10 percent year over year (Heney 2020). The most recent US Department of Defense *Annual Report on China* (United States 2020b, 128) has conceded that these investments have allowed China to develop greater ship-building capabilities, longer-range air missiles, faster anti-ship hypersonic missiles, and purchase superior integrated air defence systems (such as the Russian-imported S-400). It has also developed quantum communications and moved quickly on developing artificial intelligence.

Perhaps most worryingly, the PRC has developed a Military-Civilian Fusion development strategy that addresses the issue of civilian leadership (as opposed to military leadership) in the information technologies sector. As part of this strategy, China's defence industrial base will be fused with its civilian technological and innovation base – and harnessing the automation of the 5G-enabled Fourth Industrial Revolution to do so. The Military-Civilian Fusion doctrine also emphasizes the integration of science and technology innovation across both the military and civilian sectors, cultivating expertise and a world-class workforce that can work in both sectors, leveraging civilian logistics capabilities for military use, and expanding its mobilization system for use during wars or crises (Dorman 2020).

Indeed, Beijing has taken advantage of both the COVID-19 crisis and the Ladakh border issue with India to use civilian infrastructure to mobilize PLA forces (Lo 2020). In May 2020, China also implemented a massive, US$1.4 trillion "new-type infrastructure" (Wang 2020) spending program on 5G infrastructure, base stations, and electric vehicle powering stations, which is intended to allow China to maintain leadership in these technologies while also making the country a "manufacturing superpower" (Pan and Chen 2021). When it comes to machine-learning, China is much less hampered by data restriction rules than other countries. Considering these developments, the PRC's military capabilities could very well leapfrog those of the West across a number of areas.

Why the Five?

One of the main debates around using the Five Eyes for technology development is that restricting technology cooperation solely to within the group risks alienating other allies, many of whom – like Japan and South Korea – are world leaders in key areas of technology. Also, there are questions about using the Five Eyes framework as opposed to one that includes other nations. For example, the UK has proposed a D10 group based on the G7, but adding India, Australia, and South Korea (Brattberg and Judah 2020); there is the Prague 5G group of nations, consisting of the NATO allies, non-NATO Five Eyes members (Australia, New Zealand), Japan, India, and South Korea; and more recently, Australia, India, and Japan have developed a trusted supply chain initiative. This paper does not seek to assert that the Five Eyes should take precedence. Rather, it makes the point that these various groups might be seen as overlapping plates of armour rather than duplications of effort.

That is not to argue that they are interchangeable, however. It is clear the Five Eyes have the most highly developed level of interaction, equipment interoperability, and highest protocols around sharing sensitive information. The Five have been doing this for decades and doing it well. To that end, robust personnel security clearance protocols, common classification stan-

dards, a common professional language, and "common-enough" legal systems facilitate technology collaboration at the most sensitive levels. The Five also share a strong strategic imperative to maintain – and increase – military interoperability in the age of digital communications, artificial intelligence, and smart sensors.

Perhaps the onion metaphor is the most appropriate here: the Five have the ability to create a "quasi-defence free trade zone" or "innovation-core" using as a starting point the National Technology Industrial Base framework – those people and organizations engaged in national security, R&D, production, and maintenance of dual-use systems to support national security objectives (Congressional Research Service 2021). It is highly unlikely that states like Japan, India, or Germany, for that matter, would be interested in pooling sovereignty to that degree.

The Five have the ability to create a "quasi-defence free trade zone" or "innovation-core."

Of course, other states may be interested in collaborating in other areas such as developing common investment screening principles, belonging to a "clean network," developing common trusted supply chains in dual-use sectors, protecting open technology standards in international bodies – such as the International Communication Union (ITU) – and collaborating in areas that use less sensitive technology. In such cases, groups like the D10 or the Prague Conference would suffice. However, for more ambitious efforts such as building advanced battle management systems, military-communications capabilities, and interoperability, the Five is the more appropriate group.[17] This is for several reasons, including the fact that the UK, Australia, and Canada already have International Traffic in Arms Regulations (ITAR) waivers and already belong to the US National Technology Industrial Base (10 U.S.C. 2501).

Deciding which technologies should be restricted to the Five and which are to be open to larger groups is beyond the scope of this paper; however, we should perhaps consider which allies the United States is most likely to fight alongside and which are merely "trusted partners." An Air Force war game known as *Doolittle Series-18* found that for optimum battlefield operations, US allies had to be integrated into new multi-domain command and control (MDC2) hardware and software from the very beginning (Gilmore 2019). The level of technology integration required to develop military capabilities, sys-

tems or sensors, and command and control (Brose 2020, 144-45) should easily fall within the Five Eyes group, with access being given to more peripheral countries post-development.

Recommendations

Create a joint technology-development forum for advanced technologies. A properly funded technology development network staffed with researchers from all Five Eyes nations could take promising technologies – some from the Five Eyes Technology Cooperation Program (TTCP), others from the civilian sector, and with leads from the 2019 Five Eyes Capabilities study – **and** foster collaborative projects, co-developing the most promising into practical products. There could be various centres within the network, perhaps located in countries that already have a strong civilian or defence lead in that sector. These could include:[18]

- An electromagnetic spectrum operations (EMSO) research centre, including electromagnetic pulse weapons.
- A cyber warfare centre (data security and cloud-computing).
- An artificial intelligence research centre (machine learning applications).
- A quantum centre (computing, communications, and radar).
- An information communications centre (5G applications, military internet-of-things, 6G, etc.).
- A space centre (GPS applications, anti-satellite weapons, all-domain command-and-control development).

Encourage specific companies to cooperate on building defensive products. One interviewee has stated that the Five could encourage specific companies to team up with the military to work on different projects: "As with the Anglo-German Typhoon [fighter] program, you need to begin with a desired platform, and then agreeing to rules about who gets to use the information, how it gets shared, controlled and applied. You need rules about how to share it. If you're a partner [in a project], you should be able to get all the data and in order to modify it to suit your requirements. You also need rules on who can export it to third parties. The best way is that everyone gets a veto on third party exports."[19]

Create a STEM scholarship fund: There is a need to encourage STEM capacity in each of the Five by providing scholarships to the next generation of undergraduate and graduate engineers, coders, and scientists. These scholarships should be reserved for citizens from within the Five, but they might be used in each other's universities.[20]

Develop cyber academies: Each of the Five should establish cyber academies to train the cyber forces of tomorrow, similar to the academies that train other defence services.

Institute regular meetings between heads of Five Eyes investment screening bodies. The heads of the Committee on Foreign Investment in the United States (CFIUS), Australia's Foreign Investment Review Board (FIRB), Innovation, Science and Economic Development Canada (ISEDC), the Investment Security Unit of the UK, and the New Zealand Treasury should meet regularly to share details about nefarious investors, lessons learned, and best practices.

Establish a Joint Integrated NTIB Council. Australia, Canada, and the UK[21] are all legally part of the National Technology Industrial Base (NTIB) of the United States but the potential of this association remains unrealized.[22] While there is an NTIB Council staffed by the US Secretaries of Defense, Energy, Commerce, and Labor, it would be useful to create a joint industrial base council and secretariat made up of senior representatives[23] from each of the Five's defence, trade, and economic ministries.

As an inter-agency group, this NTIB Secretariat could recommend harmonizing technology-transfer, reforming investment screening protocols to prevent malicious foreign investment, supporting supply chain audits, establishing a government-to-government mechanism for resolving disputes, negotiating IP-sharing,[24] and aligning export control regimes. It might also consider whether to create a sort of "Free Trade Zone" (Greenwalt 2019, 29) or "ITAR[25]-free zone" (Kliman et al. 2020, 26) amongst the Five. The Joint NTIB Council could present recommendations annually to the national leaders; one interviewee also suggested that the council could even carry out joint investment screening.[26]

Carry out a Joint 5G feasibility study: 5G is a cutting-edge technology that will provide the backbone of many as-of-yet unknown downstream technologies. It is a spin-off from the Fourth Industrial Revolution. According to one interviewee, "the lack of a 5G champion among the Five Eyes was a 'Sputnik moment.'"[27] Another interviewee notes that the power of large data sets mixed with machine-learning mean that the telecommunications system will be both one of the most important weapons systems and the battleground of the future: "We are not prepared to work collectively in the information battle space, nor are we prepared to protect our populations, our IP, or our institutions, much less carrying out offensive operations."[28] This interviewee advocates a military-grade 5G network with the hardware developed outside of the global 3GPP (Third Generation Partnership Project) standards body. He states that a national-level network might be built for US$50-60 billion, which sounds high until assessed against the US$400 billion lost per year in IP theft.[29]

Create national white lists. There should be a "white list"[30] of companies, research centres, and universities within the Five that are cleared for dual-use collaboration. An interviewee states that such lists "would have to be national in the first instance, though we'd have to agree on the sort of standards or clearance protocols we wanted to set in advance."[31] White lists could be used to remove bureaucratic red tape for those companies wanting to work with defence departments and reverse the current trend of firms leaving defence. "We need to incentivize industry to get on board."[32] Conversely, black lists could also be created for those Chinese or Russian companies that should be kept out of national economies.[33]

Create inter-agency working groups on technology standards. The Five need to align more closely on Internet protocols and within 3GPP, the International Telecommunication Union, and the International Organization for Standardization (ISO). Inter-agency, public-private working groups in technology are needed – to work with standard-setting industry associations such as the Telecommunications Industry Association, the Joint Electron Device Engineering Council, and the American National Standards Institute. These groups could also meet at the level of the Five in strategic industries. The US Department of Defense Chief Information Officer has recently established a cross-department standards team (United States 2020c) – the other four countries should replicate this effort. According to one source, "One of the key things is that if we are going to play the long game, we need to give five-nation standard-setters the resources and assets to go to these conferences well-prepared both in terms of assets and allied resources."[34]

Replicate the Defence Innovation Unit. Start-ups are developing right across the Five, not merely in Silicon Valley. While the Defence Innovation Unit (DIU) is well placed to develop links with new companies in the US market, the other four might replicate the DIU model (Kliman, FitzGerald, Lee, and Fitt 2020) in places like Cambridge, UK, or Montreal, Canada. Other countries might wish to replicate In-Q-Tel[35] (an Arlington, Virginia-based not-for-profit that invests in high-tech start-up companies that support US intelligence projects). Some companies do not and will not work on defence-related projects. Nevertheless, it is essential that civil technology is allowed to spin-out into defence applications. The In-Q-Tel (US) or Imperial College Innovation Centre (UK) are possible models for this effort.

Free up DIU venture capital resources. Section 230 of the Fiscal Year 2019 *National Defense Authorization Act* authorized $75 million funding for the National Security Investment Capital to fund hardware producers. Too much venture capital is directed toward software, which can be scaled up at almost zero marginal cost. If the other four nations can create DIU-like organizations, they should also get venture capital funding for hardware (Atkinson 2020a).

Create a trusted venture capital network at DIU. One interviewee states that there is little awareness in defence departments of innovative start-up companies and technologies. He asserts that there needs to be a body that pays attention to what is taking place in industry and has a market intelligence overview similar to that held by business consultancies: "If you create a trusted venture capital (VC) network, they would know who is who; who's trustworthy and who is not. Investors are hesitant to share among themselves so we need to create a mechanism that helps them share with the government on a regular basis."[36] The Defence Innovation Unit is trying to bring new technologies into the Department of Defense, but it is not designed to develop market intelligence. The DIU should be given the resources to do this and to develop mechanisms for engaging regularly with venture capitalists.

Create national strategic technology and economic protection task forces. There needs to be multi-agency task forces in each of the Five that protects strategic technologies from illicit smuggling, malicious foreign direct investment, technology theft, and university leakage (Joske 2018). These should be led by law enforcement, but also contain defence, counter-intelligence, trade, JCORE (Joint Committee on Research Environments), and technology experts. These task forces should also have a private-public component modelled after the National Cyber-Forensics and Training Alliance (NCFTA).[37] Representatives from these task forces could also meet annually to compare notes – at both the classified and unclassified levels – on various PRC or Russian companies, proxies, the Thousand Talents program,[38] or individuals attempting to steal valuable technologies. They could also coordinate with DIU's venture capital council.

Information, Influence, and Interference

"Wherever the readers are, wherever the viewers are, that is where the propaganda reports must extend their tentacles."

– Xi Jinping
(Xinhua 2015)

States have long used and misused information as a tool of statecraft in the pursuit of national interests, during both wartime and peacetime. While different technologies have played a major part in changing the nature and use of information, authoritarian governments have been expanding their efforts at information operations "to sway populations" (White 2019) at home and abroad. In their pursuit of this strategy, Russia and China have aimed their information operations at the social and psychological levels, widening social cleavages, delegitimizing democracies, and attempting to sway the foreign policies of subject nations. While information operations against the Five have existed since the Cold War, the onset of the "Information Age" has radically changed the operational environment, shifting the scope, the level of penetration, and the targeting capabilities of information operations.[39]

With the combining of 5G telecommunications, smart sensors, wearable devices, and big data analytics, states are developing ever-widening capabilities to collect, harvest, and respond to data for political ends (Rosenberger and Gorman 2020). As Eric Rosenbach and Katherine Mansted note in a paper for the Harvard Belfer Center, the information onslaught by authoritarian powers and nefarious actors has been successful because "democracy is built on the crucial compact that citizens will have access to reliable information and can use that information to participate in government, civic, and corporate decision-making" (Rosenbach and Mansted 2018). They note that the public square has become larger and, coupled with distress-

ing images, can rapidly sway large swaths of public opinion instantaneously, while elections – the "heart and soul of a democracy" – are increasingly vulnerable to disinformation and hacking (Office of the Director of National Intelligence 2017).

China and Russia have begun to hone their use of a large range of tools – from state-funded or guided media, to trolls and bots on social media platforms like Twitter and Facebook, to the support of fringe conspiracy groups inside the West, such as the Gray Zone website (Allen-Ebrahimian 2020) – to further their messaging, distort Western intentions, and undermine the will of political leaders and weaken public support for assertive foreign policies. In an era of phenomenal amounts of data, new technologies have allowed Russian and Chinese actors to promote their ideas and disinformation across a range of areas – from pushing blame for the COVID-19 virus outside of China, to undermining support for Western vaccines, to framing US FONOPS (freedom of navigation operations) in the South China Sea as destabilizing, to asserting that New Zealand wishes to leave the Five Eyes.

While information warfare and information operations have always played a role in military conflicts in the West, Russia and China have dramatically increased their usage during peacetime (Brandt and Taussig 2020). The explosion of data has transformed the world, and the process of knowledge discovery in data (KDD) – using data mining, machine learning, and other methods – have improved the prediction of threats. Data harvesting or web scraping has become the new method for our adversaries to collect our data.

What's the problem?

Since 2014, the information environment has become extremely challenging for Western democracies. Primarily, this change has been due to the events that followed Russia's annexation of Crimea and the subsequent deterioration in relations (Guardian 2014). From then onwards, the Russian government has carried out a broad influence campaign against the United States, the United Kingdom, and other Western states, which includes cyber-attacks on political parties and politicians, interference in electoral systems, and social media influence campaigns that seek to exacerbate social cleavages, undermine popular support for the government, and promote false information or reframe important events in international affairs.

In 2018, a US Senate Intelligence Report found that the Russian Internet Research Agency carried out a widespread campaign in the lead-up to the 2016 US election, sidelining candidates that were seen as having adversarial views towards Russia. It also consistently "used hot-button, societal divisions in the US as fodder for the content they published through social media in order to stoke anger, provoke outrage and protest, push Americans further away from each other, and ferment distrust in government institutions" (US Senate

Select Committee on Intelligence 2016). According to written testimony given to the same committee, this campaign – said to have reached 125 million Americans – continued after the election (Watts 2017).

In addition to these more widely studied tools, there are also cases where China and Russia have funded political parties, universities, and the media across the West. The think tank Australian Strategic Policy Institute (ASPI) published a study showing PRC influence and funding of Chinese-language media inside Australia (Joske, Li, Pascoe, and Attrill 2020), while the decision in June 2020 by the US to designate Chinese media as foreign missions (Ortagus 2020) revealed how those companies seek to influence Western news agencies through opaque financial deals worth millions of dollars (United States 2020d). Russia and China combined spent US$300 million interfering in democratic parties and elections more than 100 times across 33 countries.

China and Russia have funded political parties, universities, and the media across the West.

According to the Alliance for Securing Democracy, which collected this data (Rudolph and Morley 2020), the interference rate increased from two or three times a year on average pre-2014 to 15 to 30 times a year post-2014, particularly affecting right-wing or populist parties in Europe (Der Spiegel 2019). Funding in universities has also become a problem with the US Department of Education reporting that in 2019, 69 percent of US universities failed to report monetary gifts in excess of US$250,000 from China's Ministry of Education (Permanent Subcommittee on Investigations Undated). The issue of Chinese influence in Western universities has implications for both freedom of speech, identification of potential targets by the PRC, and the theft or acquisition by the PRC of dual-use intellectual property (Joske 2018).

Ways and Means

In thinking of about the current age of information competition, four characteristics of Russian and Chinese tactics are immediately apparent. First, they are based on an ideological framework that is combined with modern digital methods. This is deeply important because there remains in Western circles a reluctance to view the current competition as ideological. In fact, ideology sharpens the stakes of normal state-on-state competition and seeks to de-legitimize democracy as a system of government (Rogin 2019).

As a number of experts on China's influence operations note, the country's United Front Work Department has been reinvigorated under the leadership of Xi Jinping.[40] Xi's structural reforms have greatly expanded the organization's role inside the PRC government, while doubling the number of bureaus in order to target new groups, such as "overseas Chinese students, representative individuals in 'new media,' and the young generation of entrepreneurs and businessmen" (Mattis and Joske 2019). Xi's aspirations for the "dominant position" for socialism over capitalism can be found in one of his earliest speeches as leader to the Party cadre (Greer 2019).

United Front Work Department has been reinvigorated under the leadership of Xi Jinping.

Edward Lucas, a noted Kremlinologist, notes that opportunism characterizes many Russian disinformation operations. "There is a shared strategic approach by which various Russian agencies seek to nihilistically undermine international law and norms."[41] Even Russia's use of Western judicial systems has been opportunistic; it uses them to attack domestic critics, undermining the legitimacy of those critics in the process.[42] As Peter Pomerantzev, a British-Russian journalist, found while working in Russia's media in the 2000s, the guiding principle behind Russian information warfare is "nothing is true and everything is possible" (Pomerantsev 2014). This affects not only the operational environment of the militaries of the Five, but also has an impact on their inclination and political will to deploy military power.[43]

A second characteristic of disinformation operations is plausible deniability. Both the PRC and Russia seek to undermine any collective response by the West by denying their below-the-threshold campaigns. Thus far, Beijing has denied that its tariffs on Australian products were due to a deterioration in political relations, allowing it to control the crisis and confuse Australian elites as to possible solutions. According to some observers, floating multiple interpretations of particular situations is a consistent "feature of PRC economic statecraft operating in the 'gray zone'" (Laurenceson, Pantle, and Zhou 2020). Beijing has also anticipated criticism of its policies by framing it as "containment" (Hemmings 2018) or "Western discourse power" (Rolland 2020), while Moscow uses "black PR" or *chernyi piar* to discredit or damage the reputations of its critics (Ledeneva 2006, 7; Foxall 2020b).

A third feature of the competition is its cross-sector nature. No one agency or government department can respond to the full range of interference activities and active measures that threaten the West. Instead, governments are compelled to approach this new threat in much the way we did counter-extremism and environmentalism, with "whole-of-government" or "whole-of-society" efforts.[44]

Fourth and finally, there is the long-term effect that these attacks have on social cohesion, democratic legitimacy, and political will. One interviewee states that this brings the information conflict within the purview of defence: "Australia is about to purchase 60 Joint Strike Fighters. They are worth less than scrap metal if the adversary is able to disable our ability to communicate and discuss threats, or to deter our leaders from making decisions that might lead to the deployment of those weapons. Interference at the political level is a massive asymmetrical advantage for our opponents."[45]

Recommendations

Create a counter-interference handbook. It would be helpful for the Five to develop a handbook for dealing with Russian and Chinese interference, both inside the West and in other countries. According to one interviewee, "We are rather good at preparing our own troops for enemy psy-ops. Surely, we could do something similar for the public in a handbook, without giving away our crown jewels [the most sensitive data]."[46] Such a counter-interference handbook could guide training, education, and lessons learned in other parts of government and other friendly states. It should also use the "correct language,"[47] to disseminate PRC and Russian concepts – not merely tactics.

Harness big data. As information competition is increasingly taking place online, multiple interviewees from the Five Eyes have said we must do analytics better (i.e., invest resources and coordinate data analysis). An interviewee from the US Global Engagement Center (GEC) notes the extremely volatile and shifting nature of information: "we need to spend more on the tools that enable us to make sense of all this data."[48] The GEC operates a platform called GEC-IQ with UK buy-in. The other Five countries might also wish to become stakeholders in this platform, or build a new one: "One could create a joint Five Eyes platform with a sort of secretariat that helps facilitate and coordinate product-sharing across government and subsequently gets senior-level buy-in."[49] In turn, the platform could share its products regularly with the G7 Rapid Response Mechanism (RMM) and the European Digital Media Observatory.

Broaden military intelligence: At present, defence intelligence tends to look at the military capabilities, tactics, organization, and equipment of competitor states. It would be useful for defence intelligence to broaden its collection to Russian and Chinese *civil* and *military* information operations capabilities.

Introduce messaging campaigns for defence: While the Five are very good at joint communications campaigns in active conflicts, they should increase their work in the grey zone. Issues of departmental leadership could be decided at the National Security Council level to encourage collaboration and amplification each other's messaging campaigns.[50] For example, it is highly likely the PRC will mount an intensive information campaign against the UK in response to the latter's Carrier Strike Group in the Indo-Pacific that began in July 2021 (Olsen 2021). In anticipation of that, the Five Eyes should mount a counter-operation.

Create a joint info-ops fusion centre: The Five Eyes should create an information operations / interference fusion centre that would carry out highly classified analysis and operations.[51] A second, semi-public "excellence centre" should also be established to help disseminate work among partners like Japan, France, South Korea, and Germany (much as the National Cyber Security Centre is the public face of Government Communications Headquarters in the UK). "If you made a defence-related Five Eyes version of GEC-IQ at the tactical level, it could be very helpful. Australia could bring its understanding of the PLA, the UK could bring Russia in the Middle East, and so on."[52] The resulting analysis of PRC and Russian information operations inside third countries could help inform both policy-makers and those planning counter-messaging campaigns.[53]

Broaden the role of public affairs officers. The Five all have public affairs officers in the military who inform the public about the military and ensure that the military is accountable and transparent. Their remit could be usefully broadened in two ways. First, while maintaining transparency, they could explain to the public why we have secrecy in the military and its importance in sound decision-making. Second, they could also explain the differences between accountable militaries and opaque authoritarian ones. "We must continue to show the difference between our system and theirs, while keeping within the boundaries of public affairs."[54]

Explore legislative harmonization. In creating anti-interference and foreign agents' registration legislation, one way of developing common principles is to hold an annual Five Eyes Intelligence Committee meeting.[55] According to Andrew Hastie, former Chairman of the Australian Parliamentary Joint Committee on Intelligence and Security, "that would be a great way to harmonize the Five Eyes on the issues related to foreign interference at the legislative end. You could have annual meetings that rotate both the meeting place and the chair within the Five, discussing lessons learnt, best approaches, etc."[56]

Create a centre of excellence for conventional deterrence. A centre of excellence for conventional deterrence could be housed within the Joint Policy Bureau (which will be raised in the next section) and could produce a range of analytical products that could actively deter information opera-

tions and economic coercion. As one interviewee states, "we need to grow an expertise in non-kinetic deterrence."[57] In addition to providing a place to develop that expertise, the centre could develop deterrence measures against such non-conventional aggressive actions. Since the Five are unable to unilaterally respond to Russian or Chinese interference campaigns in kind using the same tactics, they need to develop more innovative solutions to this challenge. As one interviewee states, "The entire defense system is not designed to defend or even fight in the information domain."[58] We must impose costs on those launching hostile information operations in order to deter them from doing so.

Prohibit PRC and Russian funding of academic institutions and think tanks. Russia and the PRC have begun to use the West's own traditional media to send messages to the West's populations. Problematically, some think tanks and universities involved in the public debate about our response to Russian and Chinese actions are also taking funding from them. Often this funding is not made public or is obscured. Some of the most prestigious think tanks in the US and the UK have produced strategic messages on behalf of these states that are at odds with national interests. Think tanks and university departments that take money from the PRC or Russia should be compelled to register as agents of a foreign power, publicize their funding, and be prohibited from accepting government contracts.

Military

> *"The profound influence of sea commerce upon the wealth and strength of countries was clearly seen long before the true principles which governed its growth and prosperity were detected. To secure to one's own people a disproportionate share of such benefits, every effort was made to exclude others, either by the peaceful legislative methods of monopoly, or prohibitory regulations, or, when these failed, by direct violence."*
>
> **– Alfred Thayer Mahan (1890)**

While this paper has concentrated on hybrid warfare or grey-zone tactics, we also need to acknowledge that open warfare between the great powers has re-emerged as a possibility. In Europe, Russia has already invaded Crimea and Eastern Ukraine and threatens Europe's Eastern border. In Asia, the growth of Chinese military power has been followed by concerns that China might initiate hostilities with the Philippines (Robles and Robles 2020), Vietnam (Grossman 2019), Taiwan (Shelbourne 2021), or Japan (Nikkei Asia 2021), in order to enforce its various claims over those countries' territories.

This section recognizes that NATO is the primary framework for dealing with the first threat, and the US's alliance system in the Indo-Pacific is the primary framework for dealing with the second. In neither case is it likely or attractive for the Five Eyes to play a leading role in these potential conflicts. However, this does not mean that the Five Eyes do not have a military role to play – far from it – and it is likely that the Five could play a vital function providing intelligence in the run-up to and during any conflicts. Perhaps more significantly, the Five could "backfill" in areas where NATO and America's Asian alliances are conspicuously absent – most notably, by protecting access to the maritime system itself.

Three features make up what we might call the geopolitical nature of our age. The first of these is the consolidation of power by authoritarian leaders in post-Soviet Russia and the post-1989 People's Republic of China. Each, in their own way, seeks to challenge or modify the international rules-based system to their advantage. The second feature is the shift of economic and political power from the Atlantic area to the Indo-Pacific region, and the attendant impact on maritime-based trade, naval power, and commercial shipping routes. The third feature is the effort by the Western liberal democracies to adjust to the first two trends – and to the geopolitical strategies that China and Russia have adopted.

We argue that both Russia and China are rapidly adjusting to the shift of power from the Atlantic to the Indo-Pacific and are opportunistically using this shift to gain de facto control over vital sea lanes. This is a subtle but important shift away from the principle of *mare liberum* (open sea) to *mare clausem* (closed sea) or what Andrew Lambert, a UK scholar, has called the "continentalization" of the seas (Lambert 2018, 318-19). While there has been some pretense at diplomacy, the fact is that both states are opting to use military means to develop control over these common spaces and thus threaten international sea trade, the "essential component of wealth and security"[59] for all Five Eyes members and their allies.

What's the Problem?

Many consider the challenge that China and Russia pose to the world's maritime space a historic geopolitical moment. For context, nearly 90 percent of all global trade travels by sea – some US$14 trillion in total annual value (International Chamber of Shipping Undated). Furthermore, the growing Asian middle class, expanding inter-regional trade, and the development of modern logistics mean that the Europe-Asia (OECD Undated) and Trans-Pacific shipping routes have continued growing, while Trans-Atlantic shipping has stabilized (see the graph in UNCTAD (2017)). Kun-Chin Lin, a noted Cambridge scholar, states that "in the past two decades, the crucial change in global shipping has been the back and forth swing in the balance of traffic via the eastbound route through the Pacific and Panama Canal and the westbound route via the Indian Ocean and Suez Canal" (Lin 2019, 15).

According to a well-known industry report led by Lloyds Register Group, the global middle class will grow 40 to 50 percent from current levels, with nearly 80 percent of that growth taking place in India and China (Lloyd's Register Group, QinetiQ, University of Strathclyde 2013). In other words, there will be many more consumers in the region, such that the Indo-Pacific's purchasing power will rise eight times between now and 2030, leading to "an urbanization and industrialization on a gigantic scale not seen in human history" (Lloyd's Register Group, QinetiQ, University of Strathclyde 2013). Dozens of new cities will sprout up along trade routes, requiring port infrastructure,

MAP 1: YOKOHAMA-ROTTERDAM SEA ROUTES

Adapted from: Bekkers, Francois, and Rojas-Romagosa 2015

energy infrastructure, housing, city planning, and of course, Internet and 5G connectivity. Container shipping is predicted to increase by 50 percent between now and 2030 to meet the predicted intra-regional trade and that of growing Africa-Asia trade.

Foreseeing the implications of these trends, both Russia and China have been implementing opportunistic strategies and expansive interpretations of sovereign maritime rights. They are both challenging rights to "innocent passage" as guaranteed by Article 17, Section 3 of the UN Convention on the Law of the Sea (United Nations 1982) in both territorial waters and in exclusive economic zones. Additionally, they have been building military-based networks to gain de facto control of critical waterways upon which the Europe-Asian trade depends. NATO Secretary General Jens Stoltenberg has pointed to the danger of China and Russia adopting an increasingly cooperative approach and that their combined actions might affect the global order accordingly (Rettman 2020). Using a combination of military means, debt-trap diplomacy (saddling recipient countries with loans they can't repay), and port-infrastructure financing, China has also sought to control commercial shipping routes.

As historic guarantors of the "global commons" principle – a principle that was passed down from English and Dutch notions of common law (Buck 1998, 21-24) into the maritime legal system nearly 400 years ago[60] – the Five Eyes nations have strong incentives to maintain a "free and open" maritime trading order. As one interviewee notes, "The responsibility of the lead maritime powers is to guarantee the rules of order. All of the Five are maritime powers or virtual island states. We all depend on having access to the sea."[61]

Considering Russia

The Arctic Council predicts that the summer of 2040 will see the end of summer ice in the Arctic, opening up the waters to sea trade. This will cut the length of voyages between Northern Europe and Northeast Asia by two-fifths (Breene 2017). While many in the US increasingly view Russia as a "lesser" threat (Dobbins, Shatz and Wyne 2019, 7), it is a risk taker and seems to have developed a strategy in anticipation of the opening of the northern sea route (NSR). Since 2013, it has spent billions fortifying its presence in the Arctic with advanced radars, air defence and anti-aircraft defence systems, and air bases, which all serve as a means of securing resources and future trade routes.

Russia has argued that underwater ridges mean that it should be granted a further 1.2 million square miles of the Arctic Ocean. In 2019, Sergei Lavrov, Russia's Foreign Minister, told a conference on the Arctic: "In terms of the northern sea route, this is our national transport artery… like traffic rules. If you go to another country, you abide by their rules" (Atrasheuskaya and Foy 2019). In addition to controlling the sea lane, Moscow is also intent on using its presence in the Arctic as a staging ground for projecting power into the North Atlantic (Melino and Conley 2020).

With a power base around its Northern Fleet, Russian military assets and bases in the region are fully able to contest both the GIUK-N (Greenland, Iceland, and the United Kingdom-Norway) Gap and NATO's vital sea lines of communication between North America and Europe. Russia will establish deep water control using submarines and air forces based on the Soviet-era and new bases at Novoya Zemlya, Alexandra Land, and Kotelny Island. In terms of its war-fighting capabilities, there are increasingly worrying signs that Russia is including advanced technologies into its military capabilities, in ways that Western leaders have so far failed to give it sufficient credit (Wilson 2014). Military modernization has given the Russian military "long-range hyper-velocity missiles and rockets, highly capable special operations stealth forces, advanced air defences, electronic warfare, cyber weapons, lasers to blind satellites, anti-satellite missiles and tactical nuclear weapons" (Brose 2020, 27-29). In 2018, Russia staged its military exercise Vostok with a staggering 300,000 soldiers, 1000 aircraft, and 80 warships and auxiliaries.

Considering China

Over the past two decades, China has gone from being primarily a continental power to a maritime power, expanding its blue-water capabilities (i.e., vessels that can operate for considerable periods on the high seas, far from their home ports) (Koda 2017), while developing increasing control of the commercial levers of shipping and seaports (Kynge, Campbell, Kazin, and Bokhari 2017). In 2017, two-thirds of all container traffic passed through ports that China owns or in which it has invested – and its investment in port deals continues to increase (Kynge, Campbell, Kazin, and Bokhari 2017).

Unlike Russia's Arctic gamble, China is playing a two-pronged strategy. First, it is using the Belt and Road Initiative (BRI) to develop its political and economic control over Eurasia, a strategy foreseen by British academic Halford Mackinder.[62] Second, it is also pursuing a Maritime Silk Road, using a trade-and-development approach towards the Asia-Europe sea route. According to Peter Dutton, professor at the US Naval War College, China has chosen to use force and coercion in the first instance, and lay the groundwork for the rules after the fact.

Over the past two decades, China has gone from being primarily a continental power to a maritime power.

China has identified the Azores as an essential Atlantic hub and has thus been buying up facilities in these islands, such as abandoned US storage facilities and a French hotel in which it can base 500 troops. Notably, the Azores is key to the security of undersea cables. China plans to build an air base at Lajes on the island of Terceira.

The South China Sea links Asian manufacturing with Middle Eastern energy supplies and the European market; it is one of the world's most important trade routes with nearly US$3.37 trillion of trade transiting the waterway every year (China Power 2017). Worryingly, the PRC makes three types of claims that are contrary to the freedom of the seas: first, it has drawn straight baselines around small islets and submerged features to claim large tracts of international water; second, it makes jurisdictional claims over foreign naval vessels sailing through the waters enclosed in these baselines; and, third, it asserts the right to deny permission to foreign naval vessels to transit through an exclusive economic zone (EEZ) that goes beyond what is provided for in UNCLOS.[63]

The PRC's ability and willingness to enforce these interpretations may be a step towards the principle of *mare clause*, or "closed sea," whereby a state lays sovereignty claims over portions of the high seas. These types of claims were made over the East Indies and Pacific Ocean by Spain and Portugal, and upheld in 1454 in the *Romanus Pontifex*, a Papal Bull. Notably, China's approach is rather confused. After all, its South China Sea approach stands in contrast to its support for the open seas in the Arctic. The effect of its jurisdictional claims and extensive baselines is to extend its dominion over large stretches of international waters and as such, it is at odds with a free and open trading system (as Grotius once argued).

As one interviewee notes, China's claims are merely the "tip of the iceberg." And, as a number of states sympathize with Beijing's approach, this could lead to a dangerous ripple effect on the maritime order as other states are emboldened to put forward similar claims over portions of the high seas.[64] According to recent studies,[65] there are clear dual-usage applications of its port network, its Beidou Satellite Network, and the development of BRI recipient nations' digital infrastructure (Hemmings 2020). Indeed, Chinese law and the civil-military fusion doctrine mandate that Chinese-built infrastructure conform to military specifications, while also providing the PLA with the authority to commandeer civilian assets when necessary (Russel and Berger 2020).

China has established the Djibouti Logistics Support Facility to help with its power projection.

The current National Development and Reform Commission's Five Year Plan calls explicitly for "the construction of strategic strong points along the 21st Century Maritime Silk Road," which will "radiate into the periphery, and move us into direction of the Pacific and Indian Oceans" to serve as forward support bases for military deployment and "exert political and military influence in relevant regions" (PRC National Development and Reform Commission Undated). Consistent with this approach, China has established the Djibouti Logistics Support Facility to help with its power projection, and the US Department of Defense asserts that "the PRC has likely considered Myanmar, Thailand, Singapore, Indonesia, Pakistan, Sri Lanka, United Arab Emirates, Kenya, Seychelles, Tanzania, Angola and Tajikistan as locations for PLA military logistics facilities" (United States 2020e). The capabilities of the PRC to

deny access to this waterway can be seen in the development of its large navy and advanced anti-ship systems – including the noted hyper velocity missiles – as well as its increasing capabilities to deny the global use of space using its anti-satellite weapons.

Recommendations

The Five are not really well-poised to be turned into a formal military alliance with a mutual defence treaty and nearly all respondents interviewed have stated that further institutionalization or formalizing of the group are both unnecessary and unlikely to succeed.[66] Instead, most emphasized the fluid and flexible nature of the grouping, and noted that it could backfill in areas where there was a need. In the case of the defence of US allies in Europe and in the Indo-Pacific, there are already mechanisms (NATO, the US-Japan Alliance, the US-ROK Alliance) that fulfill these requirements. However, in the case of guarding sea lanes, there is less certainty about who does what. The Five could create an informal set of arrangements that offer them the following three functions:

1. **Monitor:** watch what the PRC and Russia are doing and track military movements and claims.
2. **Coordinate:** coordinate amongst the Five on our various policies (some are at odds with each other) and with friendly and like-minded regional states about what China and Russia are doing.
3. **Act:** organize freedom-of-navigation manoeuvres, issue joint statements, organize conferences, and carry out actions within the international legal sphere.

Create a joint defence bureau: The Five must align their policies better and could do this by creating a small defence policy bureau, hosted by one country, with *secondees* from the other four. According to one interviewee, "one could model it on the think tank concept, producing actionable analysis on hostile activity and also provide food-for-thought on potential policy options. It would not replicate intelligence analysis (description) but create actionable analysis."[67] The bureau might, for example, create "cells" that focus on threats posed by Russia and China on free trade routes in the Arctic and in the Indo-Pacific. The bureau might sit within a Defence Intelligence Fusion Centre (such as the one at RAF Wyton) and could be asked to respond urgently to unexpected events or carry out analyses of recent crises.

Create an Allied Arctic region cell: The US, Canada, and the UK might start a defence-led cell within a joint bureau to look at strategic vulnerabilities along the Arctic Northern Sea Route and analyse Russian (and Chinese) threats. The cell could produce high-level analysis that would inform the Five as they develop a common approach for the region. This cell might include

sub-regional working groups that could look at specific areas of interest. An Arctic Ocean working group might be led by Canada and a North Atlantic working group might be led by the UK, for instance. The working groups would liaise and coordinate with NATO and like-minded non-NATO member states such as Japan, Sweden, and Finland, sharing intelligence and analysis case by case.

Create an Allied Indo-Pacific unit: The US, Australia, New Zealand, and the UK might create a defence-led cell within a joint bureau to look at strategic vulnerabilities along the Indo-Pacific Southern Route and analyse Chinese forces' activities across the region. The cell could produce high-level analysis that would inform the Five as they develop a common approach for the region. This cell might include sub-regional working groups that could look at specific areas of interest. A South Asia working group might be led by the UK, Australia might lead a Southeast Asia working group, New Zealand might lead a South Pacific working group, and the US might lead a Northeast Asia working group, for example. These working groups might also liaise and coordinate with like-minded states such as Japan, South Korea, India, and Singapore, sharing analysis case by case. New Zealand's announced change of stance on Five Eyes in April 2021 might result in their less enthusiastic participation in these units.

The Five all have a vested interest in the freedom of the seas, but are constrained in their support for the idea.

Carry out "joint sails" and freedom-of-navigation operations: The Five all have a vested interest in the freedom of the seas, but are constrained in their support for the idea by their fear of the PRC's willingness to impose economic punishments on those who push back against China's ambitions (*Global Times* 2018). The Five can complicate the PRC's strategy by executing multi-flagged, or multi-vessel sails, or freedom-of-navigation manoeuvres in contested international waterways as a group and with like-minded partners. If they do so, they should use a whole-of-government approach with the foreign ministries of each reinforcing that the intent is not instability, but to maintain "free and open" access to waterways for all.

Such action would allow the Five to respond horizontally rather than vertically – i.e., moving across different sectors rather than increasing in warlike attitude – and to better counter messaging from the PRC's Ministry of Foreign Affairs. Localized messaging from public affairs officers from the various defence ministries would be insufficient[68] to deal with the PRC's strategic communications, which would assert that such manoeuvres are "destabilizing." According to one interviewee, such operations must be "executed tactically, planned operationally, and messaged strategically." *Fortis-2021*, the UK Carrier Strike Group that sailed into contested waters in the Indo-Pacific in May 2021, provides an excellent example of Five Eyes interoperability, exchange of personnel, and hardware. Russia's and China's response to the deployment will be of great interest.

Focus on presence: The Five should work on being more present in the Indo-Pacific region by increasing patrols or conducting combined exercises in high seas portions of contested waters.[69] For example, the US, Australia, the UK, and regional allies like Japan could carry out multilateral exercises that display a willingness to use these waters. The group exercises could also benefit from all of the Five coordinating their messages about any such actions.

Collective messaging and alliance support: The PRC and Russia are adept at provoking small-scale crises to weaken the resolve of individual members of the Five Eyes. A classic example of this was how the PRC used the 2001 collision between its aircraft and a US Navy EP-3 aircraft – and its subsequent control over the US air crew on Hainan Island – to put the new US administration of George W. Bush on the back foot. The likelihood of the PRC carrying out a similar operation against the UK Carrier Strike Group or Canadian vessels in the South China Sea is high and should be considered a priority issue. While this is a tactical issue, it impacts the public messaging and cohesion of the five countries.

Economics

"Although China would prefer not to use trade exchanges as leverage, strained China-Australia ties and rising anti-China sentiment in Australia would discourage economic exchanges. As three Chinese government departments have already released warnings about visiting or studying in Australia, impacts on Australia's tourism industry would be deeply felt."

– Liu Xin, Liu Xuanzun,
Global Times, July 29, 2020

For nearly 75 years – since the end of the Second World War – Western theories of liberal economics and free trade have defined the global economy. While it is true the Soviet Union offered an alternative economic model, it never became a serious rival to the United States as a global trading power and Soviet GNP never rose above its 1960 peak of 58 percent of US GNP (Office of Soviet Analysis, Directorate of Intelligence 1984). The Council for Mutual Economic Assistance (COMECON), the Eastern Bloc trade organization, was never more than a "mechanism for coordinating aid and central planning goals" (Brown 1988).

Western neoliberal economics continued to expand rapidly in the post-Cold War period, promoting open, global trade. The assumptions that led the West to integrate former adversaries into the system – in particular the mutual benefits of trade and the diplomatic importance of economic interdependence – have, in a sense, blinded the West to how trade, finance, and industrial policy might be deployed for hostile geoeconomic or coercive ends (Blackwill and Harris 2017). In some ways, this is because over the past 30 years neoliberal economists have overplayed the mutual benefits of trade, while underplaying the asymmetrical nature of those benefits (World Bank Group 2018).

Economists have also failed to adjust their assumptions to account for a new environment in which a major state-capitalist trading power, such as China, might be willing to use those asymmetries for geopolitical or strategic leverage. As Leslie Gelb noted as far back as 2010, "China has been playing the new economic game at a maestro level. Staying out of wars and political confrontations and zeroing in on business interests. Its global influence far exceeds its existing economic strength. Presently, nations do not fear China's military might; they fear its ability to give or withhold trade and investments" (Gelb 2010). While Russia also presents some similar challenges, its scale is much reduced because of its lack of global technology companies and the smaller size of its economy.

Chinese companies are now expected to work with the United Front Work Department.

What's the problem?

Trade or economic coercive measures are defined as the use of threats of negative actions against the economic interests of a state or its companies in order to compel that state to change its behaviour.[70] There are various examples of states using economic statecraft throughout history. In 1916, France, the UK, Italy, and other European powers organized the Paris Economic Conference for the Allies to discuss how to prevent a post-war reoccurrence of German economic coercive statecraft (Hirschman 1945, 58). A pre-war Italian study found that through the use of targeted dumping (Viner 1924, 52), Germany had sought to prevent Italy's own industrialization (Preziosi 1914, 35), while a French study of the same period found that "Germany made war in the midst of peace with the instruments of peace. Dumping, export subsidies, import certificates, etc. all these various methods were used not as normal methods of economic activity, but as means to suffocate, to crush, and to terrorize Germany's adversaries" (Hauser 1917, 4). In today's PRC, there is a "close party-state-military-market nexus of the political system in China, wherein corporate interests serve the political agenda of the ruling Chinese Communist Party" (Brady 2019), which allows Beijing to practice a similar form of economic statecraft.

Furthermore, Chinese companies are now expected to work with the United Front Work Department in promoting the CCP's views in their dealings (Bloomberg 2020a). As a result of this quasi-public, quasi-private model, the Five Eyes nations are vulnerable in three fundamental ways: first, our com-

panies cannot compete in strategic sectors with Chinese companies that receive state support in the form of subsidies and that have stolen intellectual property; second, they are increasingly vulnerable to the PRC's ability to punitively restrict trade or investment or impose unilateral tariffs; and third, as demonstrated by the West's inability to issue personal protective equipment during the early months of the COVID-19 pandemic, they are vulnerable to supply-chain over-dependence on China. Ultimately, the Five will have to recognize that there is a deeper issue here, one that is well beyond the remit of this paper. That deeper issue is how the assumptions of market efficiencies – those that guided strategic and economic policies over the past 30 years[71] – now require an overhaul.

Since the end of the Cold War, the Five have been particularly proactive in globalizing their economies and supply chains, and in adopting neoliberal policies in the name of market efficiency. They have forgotten that the Western partners rose as global powers by affording key sectors some level of protection. As a result of the unfair practices by state capitalists (Hirson 2019) and little or no state support for these sectors at home, we have witnessed the destruction of a number of key sectors. Take, for example, the strategically significant telecommunications equipment sector[72] (to name but only one) and the related dominance of Chinese companies in the development of 5G, the backbone of the Fourth Industrial Revolution. Australian Prime Minister Malcolm Turnbull stated that acceding to Chinese dominance in this sector was a "failure of industrial policy," leading to "the point where not one of the Five Eyes countries... have any capability in wireless technology" (Sadler 2020).

When the UK's industrial icon Marconi fell in 2005 after British Telecom chose its rivals to build telecommunications infrastructure, Peter Skyte, a national officer for Amicus, the union representing postal managers, said, "No other advanced country would allow such a strategic investment decision affecting its national infrastructure to be contracted to foreign-owned suppliers" (Wray 2005). As British scholar James Rogers states, "we don't want to run to 'base protectionism,' but we could and should think about protecting strategically important sectors that relate to the future economy – such as those advanced technologies that feed into the 4th industrial revolution – as these will have dual-use applications and will be the core of vital industries in 20 years"[73]

As the Five are increasingly discovering, the economic well-being of their nations, both individually and collectively, is increasingly a national security issue. While this paper does not argue that defence should drive trade or investment, we are now at the point where defence, foreign affairs, and trade need to be more closely aligned. Competitive tendering can no longer be the mantra driving all contract awards.

Ways and Means

The PRC's economic growth has been one of the most dramatic and sustained in world history. As China has risen in prominence as an economic power, so dependency on it for trade and economic growth has grown among its neighbours and among the Five. According to Christina Lai of Johns Hopkins University, in contrast to Western states that link sanctions to human rights transgressions, "China has publicly denied any such [economic coercive] policies while at the same time quietly pursuing them" (Lai 2017, 169). This simple denial of agency limits the ability of Western states to respond through the World Trade Organization or other traditional measures (Wong 2019). Fergus Hanson, Director of the Australian Strategic Policy Institute's International Cyber Policy Centre, states, "there is no direct correlation between the threat and the punishment. The threats are deniable allowing for greater flexibility in escalating or de-escalating and for inhibiting a target's response."[74]

As Hanson's research shows, Canada and Australia have been specifically targeted, beginning with the arrest of Huawei executive Meng Wanzhou and Australia's call for a public inquiry into the origins of the coronavirus. In the case of Canada, Chinese authorities restricted canola and meat products. The canola ban – costing the industry $1 billion – was based on allegations of "harmful organisms" found in the crop. The Canadian Food Inspection Agency was unable to identify any organisms of concern (Hanson, Currey, and Beattie 2020).

China has also applied pressure on 52 foreign companies over various issues over the past four years.

Likewise, Australian barley received an anti-dumping duty of 73.6 percent and anti-subsidy duty of 6.9 percent from the Chinese Ministry of Commerce, which also announced in August 2020 that it would launch an anti-dumping investigation into Australian wine imports. As ASPI's research indicates, China has also applied pressure on 52 foreign companies over various issues over the past four years, with 82 percent complying with Chinese state directions and issuing apologies (Hanson, Currey, and Beattie 2020). Hanson warns that sustained and prolonged exposure to economic coercion like this will fundamentally reshape the international system by undermining norms and rules around the uses of trade, which will in turn affect the national interests of all five countries.[75]

Recommendations

Fortify alliances. The number of coercive economic threats or attacks against US allies is striking and must be considered part of a larger long-term anti-alliance strategy.[76] Should China continue to launch economic threats and take punitive measures against the US and its allies, the political bonds that cement security alliances will weaken. While these attacks occur in trade and the economy, they have an effect on national security and should therefore include defence. After all, such attacks have a direct impact on the national interests by attacking political will. As one interviewee states, we need to decide on whether we should respond using a "whole-of-government" approach or a "whole-of-society" approach.[77]

Consultations and joint statements. The authors of the treaties that created NATO and ANZUS were well aware that armed attacks were not the only threats that the signatories could face. Both treaties contain wording related to threats to "political independence."[78] In Article IV of the *NATO Charter*, parties will consult with each other whenever "the territorial integrity, political independence or security of any of the Parties is threatened" (NATO 1949). In ANZUS, the Security Treaty between Australia, New Zealand, and the United States, Article III reads, "The Parties will consult together whenever in the opinion of any of them the territorial integrity, political independence or security of any of the Parties is threatened in the Pacific" (Australia 1952).

Therefore, in the case of sustained economic coercion, the defence ministers from the Five, or their deputies, should consult and discuss the nature and severity of the attack and issue a joint statement that condemns the attack and collectively supports the affected member. According to one interviewee, "The Five Eyes Alliance needs to be seen calling China out when members of that alliance are intimidated or threatened. We need to be seen to be supporting each other. It sends a very big signal to Beijing, while saying nothing only encourages China's persistent attempts to isolate each of the Five."[79]

Issue appendices to the treaties. The Five should edit existing language in the NATO and ANZUS treaties so that sustained economic warfare of a certain severity is specifically included in the Article V of NATO and Article IV of ANZUS. While the apparent dangers of PRC economic coercion might not seem to merit this inclusion, the ASPI report indicates that incidences of economic coercion are steadily increasing as China's economic power grows and that coercion will become increasingly severe. These measures should be viewed as staying ahead of and deterring the threat as it increases.

Develop conventional deterrence. While the Five Eyes is not a formal alliance, its informal – and therefore flexible – nature nonetheless allows for the Five to develop a common conventional deterrence strategy using recent strategic documents.[80] Such a strategy must be calibrated carefully along with public messaging so as to maintain public support. To that end, conventional

deterrence measures could be conditions-based: 1) they must impose a cost on a country threatening any one of the Five, 2) they must be reciprocal, and 3) they must be proportionate.

Measures could range from collectively taking China to the World Trade Organization, to imposing collective measures, and to making joint statements condemning the coercion. "Naming and shaming," with its attendant public relations costs, could potentially stay Beijing's hand over time and should embolden other states to side with the Five. Economic vulnerabilities can work in both directions (Chang 2020), so the Five must also decide how to collectively respond to an attack on a strategic industry, for example, and execute a reciprocal response. As the new battlespace no longer has a front line, there must be adequate information available to the public to explain the strategy so that the public is willing to bear its potential costs.

Create a centre of excellence for conventional deterrence. A centre of excellence for conventional deterrence could be within a joint bureau (raised in the previous section) and could produce a range of actionable analytical products that would help deter economic coercion and information operations. As one interviewee has stated, "we need to create and grow an expertise in non-kinetic deterrence."[81] The bureau could provide a place to develop that expertise, especially since the Five are unable to unilaterally impose reciprocal tariffs and non-WTO compliant measures in response to China's tariffs.

Research whole-of-government responses. Whole-of-government responses could include the de-listing of Russian and PRC companies from markets in the Five and depriving them of access to western finance. The rationale for such an action could be the former's poor accounting standards, which is well within current legal frameworks. Likewise, countries could restrict or leverage the access of Russian and Chinese oligarchs to property markets and the banking sector. As one former financier notes, "the rules are in place, but unscrupulous banks and realtors are too used to a light touch from government in applying them."[82] As this approach would involve imposing costs that are not like-for-like, countries taking this action should invite other agencies and departments to help design possible counter-responses.[83]

Use the Five as a core. While the Five are a formidable economic bloc, the group could also serve as an organizing core for other like-minded countries and regional blocs (such as the EU) (Anderlini 2020).

Institute regular meetings between heads of Five Eyes investment screening bodies. The heads of the Committee on Foreign Investment in the United States (CFIUS), Australia's Foreign Investment Review Board (FIRB), Innovation, Science and Economic Development Canada (ISEDC), the Investment Screening Unit in the UK and the Treasury of New Zealand should meet regularly to exchange notes on nefarious investors, lessons learned, and best practices.

Conduct supply chain audits. In 2018, the United States completed a serious investigation on the resiliency of its defence industrial supply chain (Interagency Task Force in Fulfillment of Executive Order 13806 2018). Given the importance of defence to national security, we suggest that the other four states also carry out defence supply chain audits to measure their levels of vulnerability. It would also be suitable for all of the Five to create supply chain, inter-agency task forces that carry out wider studies of the national economies of each and identify vulnerabilities in sensitive sectors, such as rare earth metals, critical national infrastructure, or other technology-related sectors including "Smart Cities." Those task forces could introduce coordinating policy recommendations.

Create supply chain group(s). It has been clear from the COVID-19 pandemic that many countries have begun to reconsider the dependency of their supply chains on the PRC. Australia, India, and Japan have, for example, begun the Resilient Supply Chain Initiative (RSCI) (Bloomberg 2020b). The remaining four of the Five should not only join this group, but create their own supply chain standards based on the work done in 2015 by the Five Eyes critical infrastructure initiative, known as the Critical 5 (Critical 5 2015). State support, increased R&D spending, and investment screening should also be developed for sectors such as semi-conductors, data storage, power and energy storage, health care, transportation, telecommunications, and drinking water. Such efforts could also create "white lists" of approved non-Five suppliers to help the Five expand trade beyond China and thus reduce their dependency on the PRC (Rogers, Foxall, Henderson, and Armstrong 2020).

Five-country critical investment infrastructure fund. One of the primary tools that Beijing has used to co-opt developing states is to offer infrastructure funding via the BRI. As of yet, the West has not developed a large enough response to the PRC's efforts. One interviewee suggests that the Five might each contribute a billion dollars and seek private investors, and then use those monies to balance China's infrastructure policy in the Indo-Pacific. This type of private-public investment fund could work in critical areas such as telecommunications, ports, critical energy and water supply, and digital infrastructure.[84]

Carry out a five-country free trade agreement feasibility study. In the wake of the UK's decision to leave the EU, it has sought trade agreements with Australia and the United States. It would make sense to carry out a feasibility study on the idea of implementing a free trade agreement among the Five.[85] A Democracies-Five FTA would affect both the economic side and clear the path to a common defence free trade zone, as we discussed earlier in this paper. In an age of specific markets like ASEAN, China, India, and the EU, the Five should investigate the prospects and advantages of creating their own common market.[86]

Conclusion

> *"Our adversaries and rivals engage in a continuous struggle involving all of the instruments of statecraft, from what we call peace to nuclear war. Their strategy of 'political warfare' is designed to undermine cohesion, to erode economic, political, and social resilience... their goal is to win without fighting, to achieve their objectives by breaking our willpower, using attacks below the threshold that would prompt a war-fighting response."*
>
> **– Integrated Operating Concept 2025**
> (United Kingdom 2020b)

At the start of this paper, we made an effort to take an inventory of the strengths and weaknesses of the Five Eyes in order to better understand how the grouping must change to adapt to today's threats. We are fortunate, for, as one interviewee notes, "One of the beautiful things about the Five Eyes is its origins. Not many countries could provide much to the relationship back then. That is no longer the case. However, before adding others, it makes sense to use the grouping as an organizing principle... keep it very fluid and very informal... be ready for disappointments. The Five stick together because they all emerged from a common historical moment, an unseen and unstated glue."[87]

To summarize, the Five have the following four characteristics:

1. The idea behind the Five was originally based on cryptography, intelligence-sharing, and technology co-development. This remains its core function and this paper believes that these functions should alone hold the designation "Five Eyes." Expansions or "spin-offs" of the grouping should develop other names so as to protect the brand.

2. The Five Eyes alliance is not really an alliance at all, but rather an informal, ad hoc "organizing principle," comprising many discreet groups. The nations are already tied to each other through two other formal alliances, NATO and ANZUS, and these alliances are sufficient to form the backbone of security guarantees. We do not believe a formalized agreement *is* necessary, and in fact, informality is arguably a virtue.
3. The informality of the Five allows it to create new groupings, bureaucracies, and task forces, allowing a certain latitude and flexibility in dealing with the below-the-threshold-of-conflict threats that confront each of the Five. Despite this, one interviewee notes that "we must also be mindful of the difficulty of setting up new bureaucratic structures and avoid taking too wide an approach."[88] Such new groups can be created from the top down, by political elites, or they can be self-organizing, depending on the scale of the new function. "Ultimately, if they have an important enough task, then the larger bureaucracy will listen to the new grouping and take them seriously."[89]
4. Given the complexity of the threats facing the Five, the best approach is akin to overlapping plates of armour, where the Five work with other like-minded states and organizations – such as NATO, the EU, and the Quad (the US, Australia, Japan, and India) – to build resistance. New spin-off functions that do not contain the same level of sensitive or classified activity can open themselves up to partner nations, such as Japan, the Netherlands, Norway, and so on. Membership in these spin-off groups might reflect the nature of the task at hand.

While this paper has used a variation of the DIME model, opting for a TIME model (Technology, Information, Military, and Economics), the authors believe diplomacy is vital and its disappearance from this list does not reflect a "downgrading." Instead, elements of diplomacy have been inserted in almost every other part of the model, with particular emphasis on it in the section on economics, where the PRC's economic and diplomatic coercion have often gone hand in hand.

On the other hand, the corollary of the supposed downgrading of diplomacy is that technology has been upgraded. This, we believe, *is* required. The fact is we are living through a major technology shift, a period in which the digitization and centralization of data in the military, health care (including vaccine development), finance, manufacturing, transportation, commerce, and logistics – and its exploitation through artificial intelligence – will generate a global Fourth Industrial Revolution. This revolution will affect state power, the media, how society is structured, and – through the gains of first-movers – provide an opportunity for geopolitical advantage or "leapfrogging," which both Russia and China have begun to act upon. As

the UK's *Integrated Operating Concept 2025* states, technology changes mean that "old distinctions between 'peace' and 'war', between 'public' and 'private', between 'foreign' and 'domestic' and between 'state' and 'non-state' are increasingly out of date" (United Kingdom 2020b).

It is perhaps for this reason that so many of our interviewees have developed highly complex recommendations for inclusion in the technology chapter – in contrast with those they offered for fighting economic coercion. However, the economy, too, is an area of growing importance, and one that requires new models of deterrence and new modes of alliance and alignment. In the recommendations made in this paper, we have sought to use the consultations with our experts to "trial balloon" many of the most promising ideas. We have sought to cite everyone so that they can be approached for further discussion and development of their concepts.

However, while many of the recommendations in this paper were of a high standard, not all were created equally. Some were meant to address issues of greater urgency; others were more thought out and have a greater likelihood of success. At the risk of excluding some of our experts' ideas, we briefly listed what we thought were the most promising recommendations in our executive summary while keeping the bulk for discussion and consideration at the end of each chapter. Our hope is that this paper's recommendations will foster evolution – not revolution – within the Five Eyes grouping. This evolution will take place in two ways: it will offer solutions for urgent and immediate threats (collect the low-hanging fruit) and will also open up for discussion and debate long-term structural changes within the security and defence communities of our Five nations.

About the authors

John Hemmings is a professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies, a Department of Defense regional center, and an adjunct fellow at the Center for Strategic and International Studies. Prior to this, Dr. Hemmings worked in a number of think tanks in London. He has at times prepared briefings for components of the US Department of Defense, the UK's Foreign and Commonwealth Office, the UK Cabinet Office, and has been invited to give testimony to the UK Parliament Defence Committee.

Peter Varnish, OBE, FREng is an independent electronics and weapons engineer specializing in defence and security technologies and a visiting professor at the University of Coventry. Previously, he had a long career serving in various capacities for the UK Ministry of Defence and Foreign Office. He has been the Officer in Charge of Research Establishments, led the UK's Electronic Warfare Program and Strategic Defence Programme.

Appendix: Interviews

Australia

- **Anonymous**, Australian Geospatial-Intelligence Organization, August 5, 2020
- **Anonymous**, Consultant, Australian Government, August 19, 2020
- **John Fitzgerald**, Associate Professor, University of Melbourne, August 25, 2020
- **Gordon Flake**, Chief Executive Officer, Perth USAsia Centre, University of Western Australia, August 27, 2020
- **Clive Hamilton**, Professor, Charles Sturt University, August 18, 2020
- **Fergus Hanson**, Director, International Cyber Policy Centre, Australian Strategic Policy Institute, September 1, 2020
- **Andrew Hastie**, former Chair, Parliamentary Joint Committee on Intelligence and Security, August 31, 2020
- **Rory Medcalf**, Professor, Australia National University, July 26, 2020
- **Nicholas Minchin**, former Liberal member of the Australian Senate, November 19, 2020

Canada

- **Raquel Garbers**, Dir-General, Policy, Department of National Defence, August 27, 2020
- **Charles Burton**, Senior Fellow, Macdonald-Laurier Institute, July 29, 2020
- **Jonathan Berkshire Miller**, Director of the Indo-Pacific Program and Senior Fellow, Macdonald-Laurier Institute, August 14, 2020
- **Richard Shimooka**, Senior Fellow, Macdonald-Laurier Institute, August 31, 2020

- **Elinor Sloan**, Professor, Carelton University, August 26, 2020
- **Craig Stone** (ret.), Department of National Defence, September 10, 2020

New Zealand

- **Anonymous**, Strategic Policy, Ministry of Defence, August 19, 2020
- **Rob Ayson**, Professor of Strategic Studies, Victoria University of Wellington, August 11, 2020
- **Anne-Marie Brady**, Professor, University of Canterbury, September 2, 2020

United Kingdom

- **Anonymous**, Narrative Assessment Cell, UK Ministry of Defence, Cabinet Office, August 26, 2020
- **Jonathan Eyal**, Associate Director, Royal United Services Institute, August 20, 2020
- **Edward Lucas**, Non-Resident Senior Fellow, Center for European Policy Analysis September 7, 2020
- **Alan Mendoza**, Executive Director, Henry Jackson Society, September 1, 2020
- **Jim Muir**, formerly Managing Director, Head of Equity Capital Markets, Macquarie Capital Japan, August 13, 2020
- **Charles Parton**, Senior Associate Fellow, Royal United Services Institute, August 12, 2020
- **Sir Malcolm Rifkind**, former Foreign Secretary, September 3, 2020
- **James Rogers**, Director, Research, Council on Geostrategy, September 3, 2020
- **Trevor Taylor**, Professorial Research Fellow, Royal United Services Institute, September 1, 2020
- **Geoffrey Till**, Emeritus Professor, Kings College London, September 21, 2020
- **Karin Von Hippel**, Director General, Royal United Services Institute, October 14, 2020

United States

- **Anonymous**, Congressional Staffer, August 19, 2020
- **Anonymous A**, Defense Innovation Unit, Department of Defense, August 14, 2020

- **Anonymous B**, Defense Innovation Unit, Department of Defense, August 14, 2020
- **Anonymous**, Global Engagement Center, August 24, 2020
- **Rob Atkinson**, Director, Information Technology Innovation Foundation, August 3, 2020
- **Jake Bebber**, Cryptologic Warfare Officer, US Cyber Command, US Navy, August 1, 2020
- **Zack Cooper**, Research Fellow, American Enterprise Institute, August 11, 2020
- **Peter Dutton**, former Director of the China Maritime Studies Institute, US Naval War College, September 8, 2020
- **Evan Feigenbaum**, Vice President for Studies, Carnegie Endowment for International Peace, September 11, 2020
- **Taylor Fravel**, Director of the Security Studies Program, Massachusetts Institute of Technology, September, 2020
- **Michael Green**, Senior Vice President, Asia, Center for Strategic and International Studies, August 4, 2020
- **William Greenwalt**, Non-resident Senior Fellow, Atlantic Council, August 10, 2020
- **Arthur Herman**, Senior Fellow, Hudson Institute, August 7, 2020
- **Andrew Imbrie**, Senior Fellow, Center for Security and Emerging Technology (CSET), Georgetown University, August 13, 2020
- **James Lewis**, Director, Strategic Technologies Program, Center for Strategic and International Studies, August 17, 2020
- **Inez Miyamoto**, Professor, DKI-APCSS, September 2020.
- **Mira Rapp-Hooper**, Fellow, Council of Foreign Affairs, August 6, 2020
- **Martijn Rasser**, Senior Fellow, Center for New American Security, August 13, 2020
- **Mary Rose**, Strategic Communications, USARPAC, August 26, 2020
- **Laura Rosenberger**, then-Director of the Alliance for Securing Democracy, German Marshall Fund of the United States, August 24, 2020
- **David Santoro**, Vice President and Director for Nuclear Policy, Pacific Forum, September 18, 2020
- **Richard Samuels**, Professor of Political Science, Massachusetts Institute of Technology, August 28, 2020
- **Eric Sayers**, former Adjunct Senior Fellow, Center for a New American Security, August 13, 2020

- **Kelley Sayler**, Analyst in Advanced Technology and Global Security, Congressional Research Service, August 20, 2020
- **Kori Schake**, Director, FP, American Enterprise Institute, August 5, 2020
- **Robert Spalding**, Senior Fellow, Hudson Institute, September 2, 2020
- **Scott Swift**, former Commander, Pacific Fleet, US Navy, September 9, 2020

References

Allen-Ebrahimian, Bethany. 2020. "The American Blog Pushing Xinjiang Denialism." *Axios* (August 11). Available at https://www.axios.com/grayzone-max-blumenthal-china-xinjiang-d95789af-263c-4049-ba66-5baedd087df4.html.

Anderlini, Jamil. 2020. "China Is Escalating its Punishment Diplomacy." *Financial Times* (September 22).

Anderlini, Jamil. 2021. "Western Companies in China Succumb to Stockholm Syndrome." *Financial Times* (May 4).

Arno, Nataliya, Neil Barnett, Rumena Filipova, et al. 2019. *Misrule of Law: How the Kremlin uses Western Institutions to Undermine the West.* Free Russia Foundation (June). Available at https://www.4freerussia.org/misrule-of-law/.

Aslund, Anders. 2018. *Russia's Interference in the US Judiciary*. Atlantic Council, Eurasia Center. Available at https://www.atlanticcouncil.org/in-depth-research-reports/report/russia-s-interference-in-the-us-judiciary-2/.

Atkinson, Robert D. 2020a. "Emerging Defense Technologies Need Funding to Cross 'The Valley of Death'." *Real Clear Defense* (February 15). Available at https://www.realcleardefense.com/articles/2020/02/15/emerging_defense_technologies_need_funding_to_cross_the_valley_of_death_115045.html.

Atkinson, Robert D. 2020b. "Who Lost Lucent? The Decline of America's Telecom's Equipment Industry." *American Affairs* 4, 3 (Fall). Available at https://americanaffairsjournal.org/2020/08/who-lost-lucent-the-decline-of-americas-telecom-equipment-industry/.

Atrasheuskaya, Natassia, and Henry Foy. 2019. "Polar Powers: Russia's Bid for Supremacy in the Arctic Ocean." *Financial Times* (April 27).

Australia. 1952. "Appendix B—The ANZUS Treaty." *Australia's Defence Relations with the United States*. Government of Australia. Available at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Completed_Inquiries/jfadt/usrelations/appendixb.

BBC. 2019. "Chancellor Philipp Hammond's Visit to China not Going Ahead." *BBC News*. (February 16). Available at https://www.bbc.com/news/uk-47264476.

Bekkers, Eddy, Joseph Francois, and Hugo Rojas-Romagosa. 2015. "Melting Ice Caps and the Economic Impact of Opening the Northern Sea Route." CPB Discussion Paper 307, CPB Netherlands Bureau for Economic Policy Analysis. Available at https://www.cpb.nl/sites/default/files/publicaties/download/cpb-discussion-paper-307-melting-ice-caps-and-economic-impact-opening-northern-sea-route.pdf.

Bendett, Samuel. 2017a. "Russia's Military Robots are on the Move." *The National Interest* (May 4). Available at https://nationalinterest.org/blog/the-buzz/russias-military-robots-are-the-move-20502.

Bendett, Samuel. 2017b. "Red Robots Rising." *Real Clear Defense* (December 12). Available at https://www.realcleardefense.com/articles/2017/12/12/red_robots_risin_112770.html.

Blackwill, Robert D., and Jennifer M. Harris. 2017. *War by Other Means: Geoeconomics and Statecraft*. Harvard University Press.

Bloomberg. 2020a. "Chinese Communist Party Wants Bigger Role in Private Sector." *Bloomberg News* (September 15). Available at https://www.bloomberg.com/news/articles/2020-09-16/chinese-communist-party-wants-stronger-role-in-private-sector [paywall].

Bloomberg. 2020b. "Japan, Australia, and India to Launch Supply Chain Initiative." *Bloomberg News* (August 31). Available at https://www.bloomberg.com/news/articles/2020-09-01/japan-australia-and-india-to-discuss-supply-chains-alliance [paywall].

Bowen, Andrew S. 2020. *Russian Armed Forces: Military Modernization and Reforms*. Congressional Research Service (July 20). Available at https://crsreports.congress.gov/product/pdf/IF/IF11603.

Bradley, Steven. 2020. *Securing the United States from Online Disinformation – A Whole-of-Society Approach*. PCIO Policy Proposal. Carnegie Endowment for International Peace (August 24). Available at https://carnegieendowment.org/2020/08/24/securing-united-states-from-online-disinformation-whole-of-society-approach-pub-82549.

Brady, Anne-Marie. 2019. "On the Correct Use of Terms for Understanding 'United Front Work'." *China Brief* 19, 9 (May 9). Jamestown Foundation. Available at https://jamestown.org/wp-content/uploads/2019/05/Read-the-05-09-2019-CB-Issue-in-PDFB.pdf?x74728.

Brandt, Jessica, and Torrey Taussig. 2020. *Order from Chaos: The Kremlin's Disinformation Playbook Goes to Beijing*. Brookings Institution (May 19). Available at https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/.

Brattberg, Erik, and Ben Judah. 2020. "Forget the G-7, Build the D-10." *Foreign Policy* (June 10). Available at https://carnegieendowment.org/2020/06/10/forget-g-7-build-d-10-pub-82062.

Breene, Keith. 2017. "The Arctic is Now Expected to be Ice-Free by 2040." World Economic Forum (May 17). Available at https://www.weforum.org/agenda/2017/05/the-arctic-could-be-ice-free-by-2040/.

Brose, Christian. 2020. *The Kill Chain: Defending America in the Future of High-Tech Warfare*. Hachette Books.

Brown, James F. 1988. *Eastern Europe and Communist Rule*. Duke University Press.

Buck, Susan J. 1998. *The Global Commons: An Introduction*. Island Press.

Canada. 2017. *Strong, Secure, Engaged: Canada's Defence Policy*. Government of Canada, Ministry of National Defence. Available at https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html.

Cave, Danielle, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas. 2019. *Mapping China's Tech Giants*. Australian Strategic Policy Institute (April 18).

Central Committee of the Communist Party of China and the PRC State Council. 2016a. *China's National Innovation-Driven Development Strategy*. CPC Central Committee and the State Council. Available at https://cset.georgetown.edu/wp-content/uploads/t0076_innovation_driven_development_strategy_EN.pdf.

Central Committee of the Communist Party of China and the PRC State Council. 2016b. *Outline of the National Innovation-Driven Development Strategy*. (May 19). Xinhua News Agency. Ben Murphy (trans.). Center for Security and Emerging Technology, Georgetown University. Available at file:///C:/Users/KRISTI~1/AppData/Local/Temp/t0076_innovation_driven_development_strategy_EN.pdf.

Chang, Gordon G. 2020. *China Threatens Total Economic War by Dumping Treasuries: Be My Guest.* Gatestone Institute (September 10). Available at https://www.gatestoneinstitute.org/16485/china-threatens-dumping-treasuries.

China Power. 2017. *How Much Trade Transits the South China Sea?* Center for Strategic and International Studies (October 27). Available at https://chinapower.csis.org/much-trade-transits-south-china-sea/.

Commission on the Theft of American Intellectual Property. 2017. *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*. National Bureau of Asian Research, 2017.

Congressional Research Service. 2021. "Defense Primer: The National Technology and Industrial Base." Congressional Research Service, February 3. Available at https://fas.org/sgp/crs/natsec/IF11311.pdf.

Critical 5. 2015. *Role of Critical Infrastructure in National Prosperity.* Cybersecurity and Infrastructure Security Agency (October). Available at https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-ci-national-prosperity-2015-508.pdf.

Department of Homeland Security. 2019. *Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue.* Government of the United States (October). Available at https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

Der Spiegel. 2019. "Documents link AfD Parliamentarian to Moscow." *Spiegel International* (December 4). Available at https://www.spiegel.de/international/germany/documents-link-afd-parliamentarian-to-moscow-a-1261509.html.

Dobbins, James, Howard J. Shatz, and Ali Wyne. 2019. *Russia is a Rogue, not a Peer; China is a Peer, not a Rogue.* Rand Corporation (October). Available at https://www.rand.org/pubs/perspectives/PE310.html.

Dorman, Dave. 2020. *Making the Most of It, Part II: Xi Jinping Leverages Coronavirus "War without Smoke" to Spur Digital Transformation, Test National Defense Mobilization.* Security Nexus (April). Available at https://apcss.org/nexus_articles/making-the-most-of-it-part-ii/.

Dorman, Dave and John Hemmings. 2021. "Digital Marxism Perfected in Party Theory and in State Execution." (pending).

Dziedzic, Stephen. 2021. "New Zealand Trade Minister Advises Australia to show China More 'Respect'." *ABC News* (January 27). Available at https://www.abc.net.au/news/2021-01-28/nz-trade-minister-advises-australia-to-show-china-more-respect/13098674.

Economy, Elizabeth. 2019. "Yes Virginia, China is Exporting its Model." *Asia Unbound* (December 11). Council on Foreign Relations.

Edelman, Eric, Gary Roughhead. 2018. *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission.* United States Institute of Peace.

Fildes, Nic. 2018. "How Huawei Used the UK to become a Global Giant." *Financial Times* (December 7).

Foxall, Andrew. 2020a. *Russian Kleptocracy and the Rule of Law: How the Kremlin Undermines European Judicial Systems.* Henry Jackson Society (January). Available at https://henryjacksonsociety.org/publications/russian-kleptocracy-and-the-rule-of-law-how-the-kremlin-undermines-european-judicial-systems/.

Foxall, Andrew. 2020b. *Russian "Black PR": Examining the Practice of Ruining Reputations*. Henry Jackson Society Report (November). Available at https://henryjacksonsociety.org/publications/blackpr/.

Gady, Franz-Stefan. 2016. "Russia Tests Nuclear-Capable Underwater Drone." *The Diplomat* (December 14). Available at https://thediplomat.com/2016/12/russia-tests-nuclear-capable-underwater-drone/.

Galloway, Anthony. 2020. "China's Letter Shows Australia Won't Be Let out of the Diplomatic Freezer." *Sydney Morning Herald* (November 18). Available at https://www.smh.com.au/politics/federal/china-s-letter-shows-australia-won-t-be-out-of-the-diplomatic-freezer-20201118-p56fqr.html.

Gelb, Leslie. 2010. "GDP Now Matters More than Force: A US Foreign Policy for the Age of Economic Power." *Foreign Affairs* (November / December): 35-43.

Air Force Lessons Learned. 2019. "Doolittle Series 18: Multi-Domain Operations." *LeMay Center for Doctrine, Air University Press* (February). Available at https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/LP_0003_Multi_Domain_Operations.pdf.

Global Times (@globaltimesnews). "Opinion: If #Australia provokes China more, China will fight it to the end to defend its core interests. Australian education, mining and agriculture all desire improved ties with China. Possibilities of a comprehensive confrontation are low. https://bit.ly/3eezgWC." July 8, 2020. [Twitter post.] Available at https://twitter.com/globaltimesnews/status/1280899547162689541?lang=en.

Global Times. 2018. "China Slams British Navy's South China Sea Intrusion," *Global Times* (September 6). Available at https://www.globaltimes.cn/content/1118686.shtml.

Greenberg, Andy. 2018. "White House Blames Russia for Notpetya, 'the Most Costly Cyberattack in History'." *Wired* (February 15). Available at https://www.wired.com/story/white-house-russia-notpetya-attribution/.

Greenwalt, William. 2019. *Leveraging the National Technology Industrial Base to Address Great-Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies*. The Atlantic Council. Available at https://issuu.com/atlanticcouncil/docs/leveraging_the_national_technology_.

Greer, Tanner. 2019. "Xi Jinping: Uphold and Develop Socialism with Chinese Characteristics." *Palladium Magazine* (May 31). Available at https://palladiummag.com/2019/05/31/xi-jinping-in-translation-chinas-guiding-ideology/.

Grossman, Derek. 2019. "Vietnam is the Chinese Military's Preferred Warm-up Fight." *The Diplomat* (May 15). Available at https://www.rand.org/blog/2019/05/vietnam-is-the-chinese-militarys-preferred-warm-up.html.

Grotius, Hugo. 1609/ 2004. *Mare Liberum (The Free Sea)*. Richard Hakluyt (trans.) David Armitage (ed.) Indianapolis: Liberty Fund.

Guardian. 2014. "Obama and EU Slap First Sanctions on Russia over Ukraine Crisis." *South China Morning Post* (March 7). Available at https://www.scmp.com/news/world/article/1442448/obama-and-eu-slap-first-sanctions-russia-over-ukraine-crisis.

Hanson, Fergus, Emilia Currey, and Tracy Beattie. 2020. "The Chinese Communist Party's Coercive Diplomacy." Australian Strategic Policy Institute, International Cyber Policy Centre (September 1). Available at https://www.aspi.org.au/report/chinese-communist-partys-coercive-diplomacy.

Hauser, Henri. 1917. *Les Methodes Allemagne d'Expansion Economique*, 8th edition. Paris.

Hemmings, John. 2018. "The Myth of Chinese Containment." *The Interpreter* (March 9). Available at https://hemmingsjohn.wordpress.com/2018/03/09/the-myth-of-chinese-containment/.

Hemmings, John. 2020. "Reconstructing Order: The Geopolitical Risks in China's Digital Silk Road." *Asia Policy* 15, 1 (January). National Bureau of Asian Research. Available at https://www.nbr.org/publication/reconstructing-order-the-geopolitical-risks-in-chinas-digital-silk-road/.

Heney, Paul. 2020. "Global R&D Investments Unabated in Spending Growth." *R&D World Online* (March 19). Available at https://www.rdworldonline.com/global-rd-investments-unabated-in-spending-growth/.

Hille, Katherine, Neil Buckley, Courtney Weaver, and Guy Chazan. 2014. "Vladimir Putin Signs Treaty to Annex Crimea." *Financial Times* (March 18).

Hirschman, Albert O.1945. *National Power and the Structure of Foreign Trade.* University of California Press.

Hirson, Michael. 2019. *State Capitalism and the Evolution of 'China, Inc.': Key Policy Issues for the United States. Testimony before the US-China Economic and Security Review Commission, China's Internal and External Challenges.* United States Central Command (February 7). Available at https://www.uscc.gov/sites/default/files/Hirson_USCC%20Testimony_FINAL.pdf.

Horowitz, Michael. 2018. "Artificial Intelligence, International Competition, and the Balance of Power." *Texas National Security Review* 1, 3 (May).

Horowitz, Michael, Elsa B. Kania, Gregory C. Allen, and Paul Scharre. 2018. *Strategic Competition in an Era of Artificial Intelligence.* Center for a New American Security (July). Available at https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence.

Hughes, Christopher R. 2006. *Chinese Nationalism in the Global Era.* Routledge Group.

Interagency Task Force in Fulfillment of Executive Order 13806. 2018. *Assessing and Strengthening Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States.* Government of the United States, Department of Defense (September). Available at https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF.

International Chamber of Shipping. Undated. "Shipping Fact: Shipping and World Trade: Driving Prosperity." International Chamber of Shipping. Available at: https://www.ics-shipping.org/shipping-fact/shipping-and-world-trade-driving-prosperity/.

Johnson, Dave. 2018. "VOSTOK 2018: Ten years of Russian strategic exercises and warfare preparation." *NATO Review*, December 20. Available at https://www.nato.int/docu/review/articles/2018/12/20/vostok-2018-ten-years-of-russian-strategic-exercises-and-warfare-preparation/index.html

Joske, Alex. 2018. *Picking Flowers, Making Honey.* Australian Strategic Policy Institute (October 30). Available at https://www.aspi.org.au/report/picking-flowers-making-honey.

Joske, Alex. 2020. *Hunting the Phoenix.* Australian Strategic Policy Institute (August 18). Available at https://www.aspi.org.au/report/hunting-phoenix.

Joske, Alex, Lin Li, Alexandra Pascoe, Nathan Attrill. 2020. *The Influence Environment.* Australian Strategic Policy Institute (December 17). Available at https://www.aspi.org.au/report/influence-environment.

Keller, Jared. 2019. "After Experiencing Russian Jamming up Close in Syria, the Pentagon is Scrambling to Catch up." *Business Insider* (June 3).

Kliman, Daniel, Ben FitzGerald, Kristine Lee, and Joshua Fitt. 2020. Forging an Alliance Innovation Base. Center for a New American Security [CNAS] (March). Available at https://www.cnas.org/publications/reports/forging-an-alliance-innovation-base.

Kliman, Daniel, Brendan Thomas-Noone. 2018. "How the Five Eyes can Harness Commercial Innovation." *Defense One* (July 25). Available at https://www.defenseone.com/ideas/2018/07/how-five-eyes-can-harness-commercial-innovation/150040/.

Koda, Yoji. 2017. *China's Blue Water Navy Strategy and its Implications.* Center for a New American Security (March 20). Available at https://www.cnas.org/publications/reports/chinas-blue-water-navy-strategy-and-its-implications.

Kynge, James, Chris Campbell, Amy Kazin, and Farhan Bokhari. 2017. "How China Rules the Waves," *Financial Times* (January 12).

Lai, Christina. 2017. "Acting One Way and Talking Another: China's Coercive Economic Diplomacy in East Asia and Beyond." *The Pacific Review* 31, 2.

Lambert, Andrew. 2018. *Seapower States: Maritime Culture, Continental Empires and the Conflict that Made the Modern World.* Yale University Press.

Laurenceson, James, Thomas Pantle, and Michael Zhou. 2020. *PRC Economic Coercion: the Recent Australian Experience.* Australia-China Relations Institute (September 14). Available at https://www.australiachinarelations.org/content/prc-economic-coercion-recent-australian-experience.

Le Corre, Philippe and Alain Sepulchre. 2016. *China's Offensive in Europe.* Brookings Institution. Available at https://www.brookings.edu/book/chinas-offensive-in-europe/.

Ledeneva, Alena. 2006. *How Russia Really Works: the Informal Practices that Shaped Post-Soviet Politics and Business.* Cornell University Press.

Lendon, Brad. 2018. "Russia Shows off New Weapons after Trump Summit." *CNN* (July 20). Available at https://edition.cnn.com/2018/07/20/europe/russia-new-weapons-videos-intl/index.html.

Lewis, James Andrew. 2020. "Election Interference and the Emperor's New Clothes." Commentary. Center for Strategic and International Studies [CSIS] (February 4). Available at https://www.csis.org/analysis/election-interference-and-emperors-new-clothes.

Lin, Kun-Chin. 2019. "Chapter 1: Ports, Shipping, and Grand Strategy in the Indo-Pacific." In John Hemmings (ed.), *Infrastructure, Ideas, and Strategy in the Indo-Pacific* (Henry Jackson Society Report): 15-19. Available at https://daisukybiendong.files.wordpress.com/2019/04/john-hemmings-ed-2019-infrastructure-ideas-and-strategy-in-the-indo-pacific.pdf.

Lloyd's Register Group, QinetiQ, University of Strathclyde. 2013. *Global Marine Trends 2030*. Lloyd's Register Group, QinetiQ, University of Strathclyde.. Available at https://www.futurenautics.com/wp-content/uploads/2013/10/GlobalMarineTrends2030Report.pdf.

Lo, Kinling. 2020. "China Mobilises Thousands of Troops, Armored Vehicles near Border with India." South China Morning Post (June 8). Available at https://www.scmp.com/news/china/military/article/3088093/china-mobilises-thousands-troops-armoured-vehicles-near-border.

Mahan, Alfred Thayer. 1890. *The Influence of Sea Power Upon History, 1660-1783*. Little, Brown and Co.

Mattis, Peter, and Alex Joske. 2019. "The Third Magic Weapon: Reforming China's United Front." *War on the Rocks* (June 24). Available at https://warontherocks.com/2019/06/the-third-magic-weapon-reforming-chinas-united-front/.

McKew, Molly. 2017. "The Gerasimov Doctrine." *Politico* (September). Available at https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/.

McTague, Tom. 2019. "Britain's Secret War with Russia." *The Atlantic* (December 3).

Mead, Walter Russell, and Christopher Wray. 2020. *China's Attempt to Influence US Institutions: A Conversation with FBI Director Christopher Wray*. Hudson Institute (July 7). Available at https://www.youtube.com/watch?v=6MM2N-EefW8.

Melino, Matthew, and Heather Conley. 2020. *The Ice Curtain: Russia's Arctic Military Presence*. Center for Strategic and International Studies (March). Available at https://www.csis.org/features/ice-curtain-russias-arctic-military-presence.

Mintz, Alex, and Randolph T. Stevenson. 1995. "Defense Expenditures, Economic Growth and the 'Peace Dividend': A Longitudinal Analysis of 103 Countries." *Journal of Conflict Resolution* 39, 2, (June).

Nakashima, Ellen. 2019. "US Pushes Hard for a Ban of Huawei in Europe, but the Firm's 5G Prices are Nearly Irresistible." *Washington Post* (May 29). Available at https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html [paywall].

Needham, Kirsty. 2020. "Australia Faces down China in High-Stakes Strategy," *Reuters* (September 4).

Nikkei Asia. 2021. "Japan Can Use Direct Fire to Stop Senkaku Invasion, Lawmakers Say." *Nikkei Asia* (February 26). Available at https://asia.nikkei.com/Politics/Japan-can-use-direct-fire-to-stop-Senkaku-invasion-lawmakers-say.

North Atlantic Treaty Organization [NATO]. 1949. *The North Atlantic Treaty*. NATO (April 4). Available at https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

OECD. Undated. The Ocean: Ocean Shipping and Shipbuilding. OECD. Available at: https://www.oecd.org/ocean/topics/ocean-shipping/.

Office of Soviet Analysis, Directorate of Intelligence. 1984. *A Comparison of Soviet and US Gross National Products, 1960-83: A Research Paper*. Approved for release by the CIA. Available at https://www.cia.gov/readingroom/docs/CIA-RDP85T00313R000200060004-2.pdf.

Office of the Director of National Intelligence [ODNI]. 2017. *Assessing Russian Activities and Intentions in Recent US Elections*. Intelligence Community Assessment (unclassified version, January 6). Government of the United States.

Olsen, Sam. 2021. How China will see the Royal Navy's Trip to Asia? *What China Wants* (May 3). Available at https://whatchinawants.substack.com/p/how-china-will-see-the-royal-navys.

Ortagus, Morgan. 2020. "Designation of Additional Chinese Media Entities as Foreign Missions." Press Statement. Government of the United States, Department of State (June 22). Available at https://china.usembassy-china.org.cn/designation-of-additional-chinese-media-entities-as-foreign-missions/.

Pan, Che, and Celia Chen. 2021. "China zeroes in on eight core areas for country to become manufacturing superpower." *South China Morning Post* (March 5). Available at https://www.scmp.com/tech/policy/article/3124308/chinas-two-sessions-2021-beijing-zeroes-eight-core-areas-country-become.

Pearson, Natalie Obiko. 2020. "Did a Chinese Hack Kill Canada's Greatest Tech Company?" *Bloomberg Businessweek* (June 30).

Permanent Subcommittee on Investigations. Undated. *China's Impact on the U.S. Education System*. Staff Report. United States Senate, Permanent Subcommittee on Investigations. Available at https://www.hsgac.senate.gov/imo/media/doc/PSI%20Report%20China%27s%20Impact%20on%20the%20US%20Education%20System.pdf?utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery&utm_term.

Peters, Ralph. 2016. "Vladimir Putin and the Russian Soul." *Strategika*, Issue 37. Hoover Institution.

Phillips, Tom. 2015. "China building a 'Great Wall of Sand' in South China Sea is 'provocative'." *The Telegraph* (April 1). Available at https://www.telegraph.co.uk/news/worldnews/asia/china/11508803/China-building-a-Great-Wall-of-Sand-in-South-China-Sea-is-provocative.html.

Pomerantsev, Peter. 2014. *Nothing is True and Everything is Possible: the Surreal Heart of the New Russia*. PublicAffairs.

PRC National Development and Reform Commission. Undated. *The Thirteenth Five Year Plan for Economic and Social Development of the PRC (2016-2020)*. Central Compilation and Translation Press. Available at https://en.ndrc.gov.cn/newsrelease_8232/201612/P020191101481868235378.pdf.

Preziosi, Giovanni. 1914. *La Germania alla Conquista dell'Italia* [The German Conquest of Italy] Florence.

Public Safety Canada. 2019. "Five Country Ministerial and Quintet of Attorneys General Concludes." *Bloomberg* (August 1).

Reuters, 2019. "Justin Trudeau fires Ambassador to China after remarks on Huawei case." *Reuters* (January 26). Available at https://www.reuters.com/article/us-canada-china-diplomacy/canadian-pm-fires-envoy-to-china-after-remarks-on-huawei-case-idUSKCN1PK0Q5.

Rettman, Andrew. 2020. "NATO: China-Russia Axis Threatens Western Power." *EU Observer* (June 9). Available at https://euobserver.com/foreign/148597.

Robles, Alan, and Raissa Robles. 2020. "China Would 'Seize' the Philippines in a War with the US: Former Military Chief Baustista." *South China Morning Post* (October 30). Available at https://www.scmp.com/week-asia/politics/article/3107664/china-would-seize-philippines-war-us-former-military-chief.

Rogers, James. 2020. *Core Assumptions and British Strategic Policy: Toward the Next Foreign, Security and Defence Review*. The Henry Jackson Society (January 21). Available at https://henryjacksonsociety.org/publications/core-assumptions/.

Rogers, James, Andrew Foxall, Matthew Henderson, and Sam Armstrong. 2020. *Breaking the Supply Chain: How the "Five Eyes" can Decouple from Strategic Dependency*. Henry Jackson Society (May). Available at https://henryjackson-society.org/publications/breaking-the-china-supply-chain-how-the-five-eyes-can-decouple-from-strategic-dependency/.

Rogin, Josh. 2019. "China's Efforts to Undermine Democracy are Expanding Worldwide." *Washington Post* (June 27). Available at https://www.washington-post.com/opinions/2019/06/27/chinas-efforts-undermine-democracy-are-expanding-worldwide/ [paywall].

Rolland, Nadège. 2020. *China's Vision for a New World Order*. NBR Special Report, No 83. National Bureau of Asian Research (January 27). Available at https://www.nbr.org/wp-content/uploads/pdfs/publications/sr83_chinasvision_jan2020.pdf.

Rosenbach, Eric, and Katherine Mansted. 2018. *Can Democracy Survive in the Information Age?* Belfer Center for Science and International Affairs and Harvard Kennedy School (October). Available at https://www.belfercenter.org/publication/can-democracy-survive-information-age.

Rosenberger, Laura, and Lindsay Gorman. 2020. "How Democracies can Win the Information Contest." *The Washington Quarterly* 43, 2 (Summer): 75-96.

Ross, John. 2020. "Australia Investigates Ties to China: Universities' Connections Draw Scrutiny and Criticism." *Inside Higher Education* (September 3). Available at https://www.insidehighered.com/news/2020/09/03/australia-investigates-universities-ties-china.

Rudolph, Josh, and Thomas Morley. 2020. *Covert Foreign Money: Financial Loopholes Exploited by Authoritarians to Fund Political Interference in Democracies*. Alliance for Securing Democracy. Available at https://securingdemocracy.gmfus.org/wp-content/uploads/2020/08/ASD-Covert-Foreign-Money.pdf.

Ruhlig, Tim Nicholas. 2020. *Technical Standardisation, China and the Future of the International Order: A European Perspective*. Heinrich Boll Foundation / European Union E-Paper (February). Available at https://eu.boell.org/sites/default/files/2020-03/HBS-Techn%20Stand-A4%20web-030320.pdf.

Russel, Daniel R., Blake H. Berger. 2020. *Weaponizing the Belt and Road Initiative*. Asia Society Policy Institute. Available at https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf.

Sadler, Denham. 2020. "Five Eyes Fail on Wireless Tech: Turnbull." *InnovationAus* (May 5). Available at https://www.innovationaus.com/five-eyes-fail-on-wireless-tech-turnbull/.

Schoen, Fletcher, and Christopher J. Lamb. 2012. "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference." *Strategic Perspectives* 11, June. Institute for National Strategic Studies [INSS]. Available at https://inss.ndu.edu/Media/News/Article/693590/deception-disinformation-and-strategic-communications-how-one-interagency-group/.

Shelbourne, Mallory. 2021. "Davidson: China Could Try to Take Control of Taiwan in 'Next Six Years'." *USNI News* (March 9). Available at https://news.usni.org/2021/03/09/davidson-china-could-try-to-take-control-of-taiwan-in-next-six-years.

The Economist. 2020. "Threats to Britain: Into the Grey Zone: Britain's Armed Forces Get Ready for a Revolution." *The Economist* (September 19).

Turnbull, Malcolm. 2017. *Speech introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017*. Malcolm Turnbull (December 7). Available at https://www.malcolmturnbull.com.au/media/speech-introducing-the-national-security-legislation-amendment-espionage-an.

Uhlmann, Chris. 2018. "Australian Businesses with Close Ties to China Donated $5.5m to Political Parties, Investigation Shows." *ABC News* (August 20).

United Kingdom. 2010. "Newly released GCHQ Files: UKUSA Agreement." Government of the United Kingdom, National Archives (June 25).

United Kingdom. 2019. *Joint Doctrine Note 1/19. Deterrence: The Defense Contribution*. Government of the United Kingdom, Ministry of Defence (February). Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860499/20190204-doctrine_uk_deterrence_jdn_1_19.pdf.

United Kingdom. 2020a. *RESIST Counter Disinformation Toolkit*. United Kingdom, Government Communication Service (September 29). Available at https://gcs.civilservice.gov.uk/publications/resist-counter-disinformation-toolkit/.

United Kingdom. 2020b. *The Integrated Operating Concept 2025*. Government of the United Kingdom, Ministry of Defence (September 30). Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/922969/20200930_-_Introducing_the_Integrated_Operating_Concept.pdf.

United Kingdom. 2021. *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*. Government of the United Kingdom, Cabinet Office (March 16). Available at https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

United Nations Conference on Trade and Development [UNCTAD] 2017. *Review of Maritime Transport: 2017*. UNCTAD. Available at https://unctad.org/system/files/official-document/rmt2017_en.pdf.

United Nations. 1982. Article 17, Section 3. *Convention on the Law of the Sea*. United Nations. Available at https://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

United States. 1986. *Active Measures: A Report on the Substance and Process of Anti-US Disinformation and Propaganda Campaigns*. Vol. 9630. Government of the United States, Department of State.

United States. 2018. *Summary of the 2018 National Defense Strategy of the United States of America*. Government of the United States, Department of Defense. Available at https://www.hsdl.org/?view&did=807329.

United States. 2020a. *Electromagnetic Spectrum Superiority Strategy*. Government of the United States, Department of Defense (October). Available at https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF.

United States. 2020b. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2020*. Government of the United States, Office of the Secretary of Defense (September 1). Available at https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

United States. 2020c. *Department of Defense (DoD) 5G Strategy (U)*. Government of the United States, Department of Defense (May 2). Available at https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf.

United States. 2020d. Registration Statement by China Daily Distribution Corp. NSD/FARA Registration Unit. Government of the United States, US Department of Justice (June 1). Available at https://efile.fara.gov/docs/3457-Amendment-20200601-2.pdf.

United States. 2020e. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China.* Government of the United States, Office of the Secretary of Defense. Available at https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

US Senate Select Committee on Intelligence. 2016. *Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 US Election: Volume 2: Russia's Use of Social Media with Additional Views.* 116th Congress, 1st Session, Senate Report 116-XX. Available at https://digitalcommons.unl.edu/senatedocs/4/.

Viner, Jacob. 1924. *Dumping: A Problem in International Trade.* University of Chicago Press.

Wang, Xiaosong. 2020. "New Infrastructure Can Boost Economy." *China Daily* (May 14). Available at https://global.chinadaily.com.cn/a/202005/14/WS5ebc85c0a310a8b241155809.html.

Warrell, Helen. 2020. "Defence Secretary Admits UK is Behind Adversaries." *Financial Times* (September 14).

Watts, Clint. 2017. Written Testimony, Hearing before the US Senate Select Committee on Intelligence (March 30). Available at https://www.intelligence.senate.gov/hearings/open-hearing-disinformation-primer-russian-active-measures-and-influence-campaigns-panel-i.

White, Duncan. 2019. *Cold Warriors: Writers Who Waged the Literary Cold War.* Custom House.

Wilkins, Thomas S. 2012. "'Alignment, not 'Alliance' – the Shifting Paradigm of International Security Cooperation: Toward a Conceptual Taxonomy of Alignment." *Review of International Studies* 38.

Wilson, Scott. 2014. "Obama Dismisses Russia as 'Regional Power' Acting out of Weakness." *Washington Post* (March 25).

Wohlforth, William C. 1999. "The Stability of a Unipolar World." *International Studies* 24, 1 (Summer): 5-41.

Wong, Catherine. 2019. "China Denies Block on Canadian Canola Firm is Retaliation for Meng Wanzhou Case." *South China Morning Post* (March 6). Available at https://www.scmp.com/economy/china-economy/article/2188824/china-blocks-canadian-canola-exporter-tension-sabrina-meng.

World Bank Group. 2018. *Stronger Open Trade Policies Enable Economic Growth for All.* World Bank (April 3). Available at https://www.worldbank.org/en/results/2018/04/03/stronger-open-trade-policies-enables-economic-growth-for-all.

Wray, Richard. 2005. "Marconi Dealt Fatal Blow as BT Shuts It out of 21st Century." *The Guardian* (April 29). Available at https://www.theguardian.com/technology/2005/apr/29/business.onlinesupplement.

Xi, Jinping. 2013. "Keep in Mind the Present Conditions, Grasp the General Trends, Keep an Eye on Major Events, and Work Diligently to Improve Propaganda and Ideological Work." *People's Daily* (August 21).

Xi, Jinping. 2016. *Speech at the Work Conference for Cybersecurity and Informationization.* Rogier Creemers (ed. and trans.). China Copyright and Media (April 19). Available at https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/.

Xinhua. 2015. "Xi Jinping Visits the People's Liberation Army Newspaper and Delivers a Speech." [In Chinese.] *Xinhua* (December 26). Available at http://www.xinhuanet.com/politics/2015-12/26/c_1117588434.htm.

Zhang, Ketian V. 2019. *Chinese Non-Military Coercion—Tactics and Rationale.* Brookings Institution. January 2019. Available at https://www.brookings.edu/articles/chinese-non-military-coercion-tactics-and-rationale/.

Zoellick, Robert B. 2005. *Whither China: From Membership to Responsibility.* Remarks to National Committee on US-China Relations (September 21). Available at https://2001-2009.state.gov/s/d/former/zoellick/rem/53682.htm.

Endnotes

1 This is predicted by hegemonic stability theory. See, for example, Wohlforth 1999.

2 See, for example, Peters 2016, and Hughes 2006.

3 This report uses former Australian Prime Minister Malcolm Turnbull's "three c's" definition noting that interference is differentiated from influence by its coercive, corrupting, and covert nature.

4 Article V specifically states that if a NATO ally is the victim of an armed attack, every other member of the alliance will consider this an armed attack against all members and will take action to assist the ally so attacked. See https://www.nato.int/cps/en/natohq/topics_110496.htm.

5 Raquel Garbers, Director General, Strategic Defence Policy, DND (Canada), telephone meeting, August 13, 2020.

6 Eric Sayers, Adjunct Senior Fellow, CNAS (United States), telephone interview, August 13, 2020.

7 For example, lawmakers Sam Dastyari and Shaoquett Moselmane have been implicated in supporting Chinese foreign policy preferences in exchange for funding, while Andrew Robb, a former trade minister who oversaw the China-Australia free trade deal, took a six-figure consultancy role with the Chinese Belt and Road Initiative-affiliated company that took over Darwin Port immediately after he left parliament.

8 An example of an informal alliance is one where there is no charter document or treaty, but there is an understanding that a defence obligation exists and that to not fulfill it would adversely affect the relationship. The US-Israel relationship might be viewed as an informal alliance.

9 While there are questions about New Zealand's adherence to ANZUS, it has never, in fact, withdrawn from the treaty.

10 The 1943 BRUSA Agreement or the 1946 UKUSA Agreement might each be considered a founding treaty to the intelligence relationship, but neither adequately covers the areas that have since fallen under the Five Eyes purview over time.

11 Michael J. Green, Senior Vice President, Center for Strategic and International Studies (United States), telephone interview, August 4, 2020.

12 Raquel Garbers, Director-General, Strategic Defence Policy, Department of National Defence (Canada), telephone interview, August 27, 2020.

13 Rob Ayson, Prof of Strategic Studies, Victoria University of Wellington (New Zealand), telephone interview, August 11, 2020.

14 The Quadrilateral group consists of the US, Australia, Japan, and India.

15 For example, the top five artificial intelligence companies in the US – Amazon, Alphabet, Facebook, Microsoft, and Apple – spent US$70 billion on R&D while the top five defence companies – Lockheed Martin, Boeing, Raytheon Technologies, General Dynamics, and Northrup Grumman – spent only US$6.2 billion.

16 Such as the 14th Five-Year plan (2016-2020), *Digital China, New Type Infrastructure Action Plan, Made in China: 2025*, the National Innovation-Driven Development Outline, and the Next Generation Artificial Intelligence Development Plan.

17 As ever, every rule requires an exception. While the authors do not believe that Japan, Taiwan, or South Korea should be included in the intelligence part of the Five Eyes, there will be cases when we must collaborate closely with them in critical technologies – such as semi-conductors and stealth materials – which can be handled through bodies like the US-Japan Systems and Technology Forum or the UK-Japan Agreement on Transfer of Arms and Military Technologies.

18 The question of which technologies should be the focus of the Five's efforts could be decided collectively or by examining the nine technologies put forward in the US Third Offset Strategy and the 2018 National Defense Strategy.

19 Trevor Taylor, Professorial Research Fellow, Royal United Services Institute (RUSI) (UK), telephone interview, September 1, 2020.

20 Rob Atkinson, Director, ITIF (US), telephone interview, August 3, 2020.

21 New Zealand should decide if it wishes to be included and if this is an effort in which it wishes to take part. This paper strongly supports its inclusion. If New Zealand wishes to take part in the NTIB, the others should make an effort to include it.

22 Arthur Herman, Senior Fellow, Hudson Institute (US), telephone interview, August 7, 2020.

23 William Greenwalt recommends a person at the Deputy Assistant Secretary level in the United States to help ensure that the wider government takes the council's recommendations seriously.

24 Elinor Sloan, Professor, Carleton University (Canada), telephone interview, August 26, 2020.

25 International Traffic in Arms Regulations.

26 Rob Atkinson, Director, ITIF (US), telephone interview, August 3, 2020.

27 Senior staffer, US Congress, telephone interview, August 19, 2020.

28 Robert Spalding, Senior Fellow, Hudson Institute (US), telephone interview, September 2, 2020.

29 Robert Spalding, Senior Fellow, Hudson Institute (US), telephone interview, September 2, 2020.

30 Kori Schake, Director, Foreign and Defense Policy, American Enterprise Institute (AEI) (US), telephone interview, August 5, 2020.

31 Trevor Taylor, Professorial Research Fellow, RUSI, telephone interview, September 1, 2020.

32 Andrew Imbrie, Senior Fellow, Center for Security and Emerging Technology (CSET), Georgetown University, telephone interview, August 13, 2020.

33 Arthur Herman, Senior Fellow, Hudson Institute (US), telephone interview, August 7, 2020.

34 Andrew Imbrie, Senior Fellow, CSET, Georgetown University (US), telephone interview, August 13, 2020.

35 Martijn Rasser, Senior Fellow, Center for a New American Security (CNAS) (US), August 13, 2020.

36 William Greenwalt, Senior Fellow, AEI (US), telephone interview, August 10, 2020.

37 Inez Miyamoto, Professor, DKI-APCSS (US), telephone interview, September, 2020.

38 For a recent report on the Thousand Talents program, see Joske 2020.

39 This is defined in its broadest sense to mean uses of information to influence, corrupt, usurp, or socially disrupt for political ends rather than the traditional meaning found in military doctrine.

40 Anne-Marie Brady, Professor, University of Canterbury (New Zealand), telephone interview, September 2, 2020.

41 Edward Lucas, Non-Resident Senior Fellow, Center for European Policy Analysis, telephone interview, September 7, 2020.

42 See, for example, Arno, Barnett, Filipova, et al. 2019, Foxall 2020a, and Aslund 2018.

43 Anonymous, Consultant to the Australian government, telephone interview, August 19, 2020.

44 See, for example, Department of Homeland Security 2019, and Bradley 2020.

45 Anonymous, Consultant to Australian Government, telephone interview, August 19, 2020 and United Kingdom 2020a.

46 Edward Lucas, Non-Resident Senior Fellow, Center for European Policy Analysis (UK), telephone interview, September 7, 2020.

47 Anne-Marie Brady, Professor, University of Canterbury (NZ), telephone interview, September 2, 2020.

48 Anonymous, Global Engagement Center (US), telephone interview, August 1, 2020.

49 Raquel Garbers, Director-General, Strategic Defence Policy Department of National Defence (Canada), telephone interview, August 27, 2020.

50 An example of allied messaging to counter Russian disinformation occurred when US and NATO troops deployed in the Baltic states as part of the European Reassurance Initiative.

51 Edward Lucas, Non-Resident Senior Fellow, Center for European Policy Analysis (UK), telephone interview, September 7, 2020.

52 Major Jon Hassain, MBE, Narrative Assessment Cell, Ministry of Defence, Cabinet Office (UK), telephone interview, August 26, 2020.

53 Anne-Marie Brady, Professor, University of Canterbury (NZ), telephone interview, September 2, 2020.

54 Edward Lucas, Non-Resident Senior Fellow, Center for European Policy Analysis (UK), telephone interview, September 7, 2020.

55 This would include the US Select Committees on Intelligence, the UK's Intelligence and Security Committee of Parliament, the New Zealand Intelligence and Security Committee, the Australian Parliamentary Joint Committee on Intelligence and Security, and Canada's National Security and Intelligence Committee of Parliamentarians.

56 Andrew Hastie, former Chair, Parliamentary Joint Committee on Intelligence and Security (Australia), telephone interview, August 31, 2020.

57 David Santoro, Vice President and Director for Nuclear Policy, Pacific Forum (US), telephone interview, September 18, 2020.

58 Robert Spalding, Senior Fellow, Hudson Institute (US), telephone interview, September 2, 2020.

59 Peter Dutton, former Director of the China Maritime Studies Institute, US Naval War College, telephone interview, September 8, 2020.

60 Hugo Grotius' 1609 book *Mare Liberum* (The Free Sea) was in response to the Portuguese policy of *Mare Clausum* (Closed Sea), in which Grotius argued that counter to Portugal's claims to a monopoly for trade in the East Indies, the sea was free to all: "Every nation is free to travel to every other nation, and to trade with it" (Grotius 1609/2004, 7).

61 Admiral Scott Swift (ret.), former Commander, Pacific Fleet, US Navy, telephone interview, September 9, 2020.

62 Mackinder founded the term *geopolitics*, while also putting forward his theory that any power that dominated the "Heartland" could come to dominate the World-Island, linking the continents of Europe, Asia, and Africa.

63 Peter Dutton, former Director of the China Maritime Studies Institute, US Naval War College, telephone interview, December, 2019.

64 Geoffrey Till, Emeritus Professor, Kings College London (UK), telephone interview, September 21, 2020.

65 See for example, Russel and Berger 2020.

66 Those opposed include Sir Malcolm Rifkind, former Foreign Secretary (UK); Rory Medcalf, Professor at Australia National University; Scott Dewar, Director of Australian Geospatial-Intelligence Organization and formerly with Australia's Department of Defence; Jonathan Eyal, Associate Director, Royal United Services Institute (UK); Michael J. Green, Senior Vice President, Center for Strategic and International Studies (US); Mira Rapp-Hooper, Fellow, Council of Foreign Affairs (US); and Admiral Scott Swift, former Commander, Pacific Fleet (US).

67 Raquel Garbers, Director-General, Strategic Defence Policy Department of National Defence (Canada), telephone interview, August 27, 2020.

68 Admiral Scott Swift, USN (ret.), former Commander, Pacific Fleet, telephone interview, September 9, 2020.

69 M. Taylor Fravel, Professor, MIT, telephone interview, September 25, 2020.

70 This borrows from Ketian Zhang's definition in his 2019 *Chinese Non-Military Coercion – Tactics and Rationale*.

71 See Rogers (2020) for a critical discussion of the assumption that "globalization is an immutable and desirable force."

72 For example, see Atkinson 2020b, Pearson 2020, Fildes 2018, and Wray 2005.

73 James Rogers, Director, Council for Geostrategy, telephone interview, September 3, 2020.

74 Fergus Hanson, Director, International Cyber Policy Centre, Australian Strategic Policy Institute (ASPI), telephone interview, September 1, 2020.

75 Fergus Hanson, Director, International Cyber Policy Centre, ASPI (Australia), telephone interview, September 1, 2020.

76 As of writing, all five nations have had trade threats levelled against them through various Chinese media, such as *Global Times*, over such issues such as blocking Huawei in national 5G infrastructure or freedom of navigation manoeuvres in the South China Sea. Canada and Australia have suffered actual punitive measures.

77 David Santoro, Vice President and Director for Nuclear Policy, Pacific Forum (US), September 18, 2020.

78 This directly relates to the growing view inside Australia that China poses a threat to its democracy and its national sovereignty. See Needham 2020.

79 Nicholas Minchin, former Liberal member of the Australian Senate, November 19, 2020.

80 See, for example, United Kingdom 2019.

81 David Santoro, Vice President and Director for Nuclear Policy, Pacific Forum (US), September 18, 2020.

82 Jim Muir, former Managing Director, Head of Equity Capital Markets, Macquarie Capital Japan, August 13, 2020.

83 David Santoro, Vice President and Director for Nuclear Policy, Pacific Forum (US), September 18, 2020.

84 Evan Feigenbaum, Vice President for Studies, Carnegie Endowment for International Peace (US), September 11, 2020.

85 Rob Atkinson, President, Information Technology Innovation Foundation (US), telephone interview, August 3, 2020.

86 Some suggest that the UK appetite for new free trade agreements is low. In fact, the opposite is true. UK attitudes toward the EU soured over the political aspects of the arrangement, not the common market aspect, which was historically London's preference.

87 Jonathan Eyal, Associate Director, Royal United Services Institute (UK), telephone interview, August 20, 2020.

88 Karin von Hippel, Director General, Royal United Services Institute, telephone interview, October 14, 2020.

89 Karin von Hippel, Director RUSI, telephone interview, October 14, 2020

MACDONALD-LAURIER INSTITUTE

TRUE NORTH IN CANADIAN PUBLIC POLICY

excellent

THOUGHT-PROVOKING

> Canada shall be the star towards which all men who love progress and freedom shall come.
>
> – Sir Wilfrid Laurier

CONSTRUCTIVE important insightful

Critically acclaimed, award-winning Institute

The **Macdonald-Laurier Institute** focuses on the full range of issues that fall under Ottawa's jurisdiction.

- Winner of the Sir Antony Fisher International Memorial Award (2011)
- Templeton Freedom Award for Special Achievement by a Young Institute (2012)
- Prospect Magazine Award for Best North America Social Think Tank (2018)
- Short-listed for the Templeton Freedom Award (2017).
- Cited by five present and former Canadian Prime Ministers, as well as by David Cameron, then British Prime Minister.
- *Hill Times* says **Brian Lee Crowley** is one of the 100 most influential people in Ottawa.
- *Wall Street Journal*, *Economist*, *Foreign Policy*, *Globe and Mail*, *National Post* and many other leading publications have quoted the Institute's work.

WHERE YOU'VE SEEN US

CTV · cpac FOR THE RECORD · Corus ENTERTAINMENT · CBC news · FP Foreign Policy · tvo · The Economist · WALL STREET JOURNAL · THE HILL TIMES · THE GLOBE AND MAIL · NATIONAL POST

macdonaldlaurier.ca

MACDONALD-LAURIER INSTITUTE

MLI

TRUE NORTH
IN CANADIAN PUBLIC POLICY

WHAT DO WE DO?

At **MLI**, we believe ideas matter. The Macdonald-Laurier Institute is the only non-partisan, independent public policy think tank in Ottawa focusing on the full range of issues that fall under the jurisdiction of the federal government. We are the leading platform for the best new policy thinking in the country. And our goal is to be an indispensable source of reasoned and timely thought leadership for policy-makers and opinion leaders, and thereby contribute to making Canada the best governed country in the world.

SIR JOHN A. MACDONALD

SIR WILFRID LAURIER

WHAT IS IN A NAME?

The **Macdonald-Laurier Institute** exists to renew the splendid legacy of two towering figures in Canadian history:

Sir John A. Macdonald
and **Sir Wilfrid Laurier.**

A Tory and a Grit, an English speaker and a French speaker, these two men represent the very best of Canada's fine political tradition. As prime minister, each championed the values that led to Canada assuming her place as one of the world's leading democracies. We will continue to vigorously uphold these values, the cornerstones of our nation.

PROGRAM AREAS

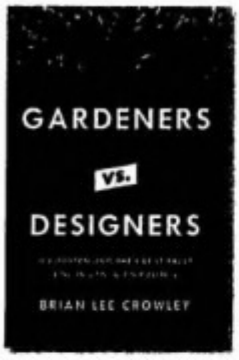
The Institute undertakes an impressive program of thought leadership on public policy. Some of the issues we have tackled recently include:

- Building Canada's energy advantage;
- Achieving reconciliation with Indigenous peoples;
- Making Canada's justice system more fair and efficient;
- Defending Canada's innovators and creators;
- Controlling government debt at all levels;
- Advancing Canada's interests abroad;
- Regulating Canada's foreign investment; and
- Fixing Canadian health care.

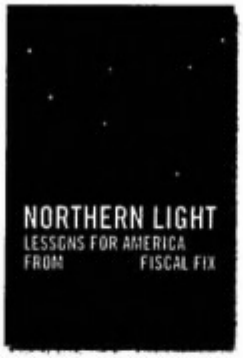
macdonaldlaurier.ca

MACDONALD-LAURIER INSTITUTE PUBLICATIONS

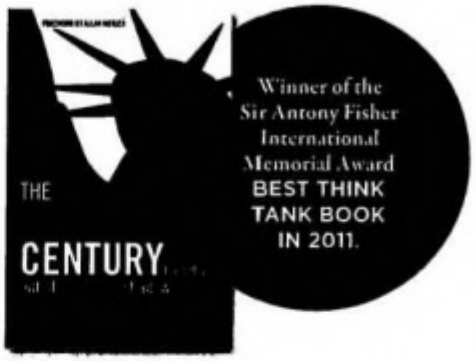
BOOKS



Gardeners vs. Designers
Brian Lee Crowley



Northern Light
Brian Lee Crowley, Robert P. Murphy, Niels Veldhuis

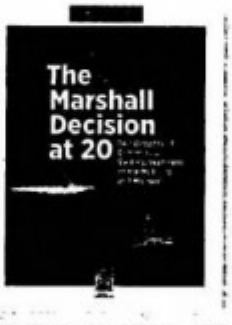


The Canadian Century
Brian Lee Crowley, Jason Clemens, Niels Veldhuis

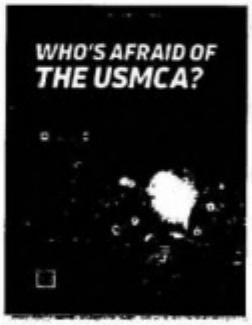
HIGHLIGHTS OF OUR PUBLICATIONS PROGRAM OVER THE YEARS

Ending Pakistan's Proxy War in Afghanistan
Chris Alexander

Countering China's Economic Coercion
Duanjie Chen



The Marshall Decision at 20
Ken Coates

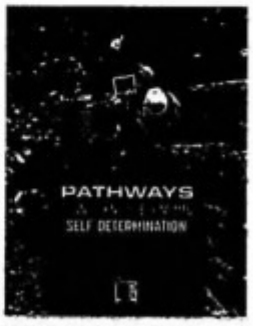


Who's Afraid of the USMCA?
Richard C. Owens

Facing the Authoritarian Challenge
Balkan Devlen

The Clean Fuel Regulation: Who Needs It?
Dennis McConaghy, Jack Mintz, Ron Wallace

Turning the Channel on Cancon
Jill Golick, Sean Speer



Pathways to Indigenous Economic Self-Determination
Heather Exner-Pirot

Ideas change the world

WHAT PEOPLE ARE SAYING ABOUT MLI

The Right Honourable
Paul Martin

I want to congratulate the **Macdonald-Laurier Institute** for 10 years of excellent service to Canada. The Institute's commitment to public policy innovation has put them on the cutting edge of many of the country's most pressing policy debates. The Institute works in a persuasive and constructive way to present new and insightful ideas about how to best achieve Canada's potential and to produce a better and more just country. Canada is better for the forward-thinking, research-based perspectives that the **Macdonald-Laurier Institute** brings to our most critical issues.

The Honourable
Jody Wilson-Raybould

The **Macdonald-Laurier Institute** has been active in the field of Indigenous public policy, building a fine tradition of working with Indigenous organizations, promoting Indigenous thinkers and encouraging innovative, Indigenous-led solutions to the challenges of 21st century Canada. I congratulate **MLI** on its 10 productive and constructive years and look forward to continuing to learn more about the Institute's fine work in the field.

The Honourable
Irwin Cotler

May I congratulate **MLI** for a decade of exemplary leadership on national and international issues. Through high-quality research and analysis, **MLI** has made a significant contribution to Canadian public discourse and policy development. With the global resurgence of authoritarianism and illiberal populism, such work is as timely as it is important. I wish you continued success in the years to come.

The Honourable
Pierre Poilievre

The **Macdonald-Laurier Institute** has produced countless works of scholarship that solve today's problems with the wisdom of our political ancestors. If we listen to the **Institute**'s advice, we can fulfill Laurier's dream of a country where freedom is its nationality.

MACDONALD-LAURIER INSTITUTE

MLI
TRUE NORTH
IN CANADIAN PUBLIC POLICY

323 Chapel Street, Suite 300,
Ottawa, Ontario K1N 7Z2
613-482-8327 • info@macdonaldlaurier.ca

@MLInstitute
facebook.com/MacdonaldLaurierInstitute
youtube.com/MLInstitute
linkedin.com/company/macdonald-laurier-institute