



UNSW
A U S T R A L I A

Australian Centre for
Cyber Security

UNSW Canberra

Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security

Greg Austin, Ph D

Prepared for

Session on The Global Cybersecurity Environment

Author Note

Professor Greg Austin is an international security specialist recently appointed at the Australian Centre for Cyber Security (ACCS) in the University of New South Wales Canberra. He concurrently serves as a Professorial Fellow at the EastWest Institute, an NGO with key offices in New York, Brussels and Moscow. He is the author of *Cyber Policy in China* (Polity: Cambridge 2014), the first comprehensive study of China's response to the information age addressing political, economic, military and diplomatic aspects. As a Vice President of EastWest in 2009, Austin was co-founder with the late John Mroz, then CEO of EastWest, of the Worldwide Cybersecurity Initiative, now in its seventh year and re-badged under new leadership to focus on cyberspace cooperation. Austin is the author of a number of articles and papers on international security impacts of the information age, as well as several books or longer studies on the security policies of China, Taiwan, Japan, and Russia. His thematic interests include preventive diplomacy, energy security, countering violent extremism and ethics. He served in Australian defence intelligence for more than a decade. He has held appointments as a Ministerial Adviser, Secretary of a Senate Committee, and Canberra-based correspondent for the *Sydney Morning Herald*. During 15 years working in Europe, including seven years with EastWest, Austin held senior roles in the International Crisis Group, the Foreign Policy Centre London, and the renowned Peace Studies Department at Bradford University. He has also worked as a consultant for the UK Cabinet Office, the UK Ministry of Defence, the European Commission, the BBC, and the Australian Department of Foreign Affairs. He has held academic posts in the Australian National University and a Senior Visiting Fellowship in the Department of War Studies at King's College London. He has a Ph D and Master's Degree in International Law.

ABSTRACT

The response by middle powers to the emerging centrality of cyber space in the conduct of future war has been slow and fragmented. Their cyber war play-books are not blank but they look very different from those of pace-setter countries. This paper describes a number of international benchmarks which might provide guideposts for a rapid catch-up in middle power capabilities for military security in the information age (for cyber-enabled war).

On the one hand, the paper looks at the future international policy environment. It calls out major trends in the policy settings of two pacesetter countries: China and the United States. Both regard military dominance in cyber space as one of the primary determinants of success in war. Few governments among the middle powers have been prepared to canvas in public the centrality of cyber-enabled warfare or craft policies and doctrines accordingly. The discussion of the policies of China and the United States lays the foundation the paper's review of international trends in war avoidance (preventive diplomacy) and middle power needs to shape those developments. The United States and China have taken decisions in 2015 that reveal their determination to race ahead to the next stage of development of cyber arsenals. They seek to create conditions in cyber space that in war time could undermine the effectiveness of the weapons systems, deployed units and military-related civil infrastructure of an enemy as quickly as possible. The two major powers are placing considerable attention on disabling enemy cyber systems in the early stages of hostilities, or even on a pre-emptive basis.

On the other hand, the paper previews trends in the technologies and characteristics of cyber-enabled war (attack technologies and defensive systems) and complex cyber-enabled war scenarios. These trends are moving in a direction that will present almost insurmountable challenges to the security of most middle powers. These countries will need to develop complex responsive systems of decision-making for medium intensity war that address multi-vector, multi-front and multi-theatre attacks in cyber space, including against civilian infrastructure and civilians involved in the war effort. Middle power defence forces will need to maintain distinct capabilities for cyber warfare at the strategic level. The capabilities need to be unified in both policy and doctrinal terms in a way that lays a clear pathway for mobilization of each country in very short time to fight a medium intensity, cyber-enabled hot war. This will require new technologies of decision-making that do not yet exist in most G20 countries.

The paper recommends that interested middle powers build a much more visible community of interest around the concept of cyber-enabled warfare with a recognised authoritative hub (a global cyber warfare studies centre) that can unite political, military, diplomatic, business, scientific and technical interests and expertise. The NATO Centre for Cyber Defence can be a strong partner in this but the NATO alliance framework places some constraints on its potential role. In the next two decades, the war-fighting needs of middle powers in cyber space, as for their counter-terrorism needs, cannot be met without considerable dilution of pre-existing alliance and blocs and more effective bridging of the big geopolitical divides. Collective security in cyberspace may be the only answer for middle powers.

Contents

Introduction	1
National Security Needs in Cyber Space: Information Dominance.....	2
International Trends in Planning for Cyber-enabled War.....	5
Cyber Military Policy in China	5
Cyber Military Policy in the United States.....	8
War Avoidance and Peace Building.....	11
Cyber War: Trends and Technologies	14
Special Features of Cyber War.....	17
Future Systems of Attack and Defence	19
Technologies of Decision-making.....	21
Scenario Planning for Cyber-enabled War.....	22
Conclusion and Recommendations.....	24
References	26

Introduction

For a quarter of a century, middle power governments have been outclassed by more nimble small powers in coming to terms with the full import of the digital revolution transforming the world. This consistent edge of certain small powers has been captured in the annual Network Readiness Index prepared for the World Economic Forum, the 2015 version of which saw Singapore and Finland ranked yet again at the forefront (1 and 2), ahead of Sweden, the Netherlands and Norway (at 3.4 and 5), with no G20 countries in top five.¹ This laggardness in cyber readiness among most middle powers has been particularly visible in the defence sector even though world's only superpower, the United States, began a clear transition in its cyber military ambitions in the mid-1990s. For example, in the India case, in 2012, an IDSA Task Force recommended that "India must raise a cyber command".² By August 2015, the Times of India reported that the Modi government was preparing to implement the recommendation, but the newspaper observed that "India has been quite slow to respond to the ever-expanding military challenges and threats in space and cyberspace".³

There has been little effort in public by middle power governments to benchmark national security needs in cyber space in the same way as they benchmark naval, air and ground capability against strategic needs (strengths and weaknesses of potential enemies and their intentions) and balance those against national budget constraints. Most of these countries have high profile national debates about whether they need a sovereign capability to build naval combat ships, submarines, fighter aircraft but have been relatively silent on the type of national cyber innovation system they need for future warfare. To help stimulate such a debate, this paper attempts to use a benchmarking approach across a combined set of political, economic, military and technical issues.

While recognising the limitations of benchmarking, the paper sees the value of such an exercise as helping to evaluate a country's current levels of performance, build political pressure for change, identify gaps, expose other countries' pathways to success, and find innovative approaches.⁴

The first main section of this paper lays out selected aspects of what two countries of high strategic interest—China and the United States—have done or may be planning to do in the 10-20 year time frame. Second, the paper previews trends and characteristics of cyber-enabled war, systems for attack and defence, asymmetric warfare, distributed warfare, and scenario planning. In summary, the benchmarks reviewed in the paper are derived from the sources listed in Table 1.

¹ World Economic Forum (WEF), *Global Information Technology Report 2015*, New York: Oxford University Press, for the World Economic Forum and others, p. 8. Available at: http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf.

² Institute for Strategic and Defence Analyses, *India's Cyber Security Challenges*, a Task Force Report, 2012, p. 46, available at <http://www.idsa.in/book/IndiasCyberSecurityChallenges>.

³ "Govt Gets Cracking On Three New Tri-Service Commands", *Times of India*, 20 August 2015, carried on <http://www.defense-aerospace.com/articles-view/release/3/166156/india-plans-3-joint-commands-for-space.-cyber-and-covert-ops.html>.

⁴ Sigurdur Helgason, "International Benchmarking: Experiences from OECD Countries", Paper Presented at a Conference Organised by the Danish Ministry of Finance on International Benchmarking, Copenhagen, 20-21 February 1997, p. 2, www.oecd.org/governance/budgeting/1902957.pdf.

TABLE 1: LIST OF BENCHMARKS DISCUSSED**Future National Defence Postures**

China: cyber power intent, cyber S&T intent, distributed cyber war, militia

United States: prompt information dominance, cyber weapons for all, R&D innovation, military education

War avoidance and peace building

Future ‘Cyber-enabled war’ trendsFuture technologies of complex cyber attack and defence
(multi-vector, sustained, cyber + kinetic)

Technologies of decision-making

Scenario planning

A comprehensive study of middle power national security needs in cyber space relying on such benchmarks would require more research, expertise and time than have been available to this author. Therefore the value of this paper is more in its pointing to the need for, and potential scope of more comprehensive, public domain studies.

The discussion in the paper is introduced by a necessary review of the boundaries of the topic of “national security in cyber space” or “cyber-enabled war”, since many policy documents are not as consistent or rigorous in differentiating key aspects of this as they might be. The NATO Cyber Cooperative Defence Centre of Excellence notes: “There are no common definitions for Cyber terms - they are understood to mean different things by different nations/organisations, despite prevalence in mainstream media and in national and international organisational statements.”⁵ In many policy documents, the term “cyber security” is too often used as a catch all to avoid specific public elaboration of concepts like cyber war and cyber effect operations.

National Security Needs in Cyber Space: Information Dominance

The term “cyber war” is shorthand for a phenomenon that is not easily captured in a single term, much less one that may have shared meaning for people involved in national security policy around the world. The inadequacy of the word “cyber” as a prefix is illustrated quite well by the title of the book, *Cyber War Will Not Take Place*.⁶ The book depends in its main argument on a narrow interpretation of the term “cyber war” as one limited to operations in cyber space. As such, the argument is defensible but the number of countries actively preparing for what most of us call “cyber war” is growing. They obviously believe that something like cyber war or war in cyber space may take place. The only way to get around this lack of terminological precision in the word “cyber” is for each publication that uses it to say how it understands the term.

There has to be a clear distinction made between “cyber security” on the one hand and, on the other, discussions of military and defence needs in cyber space. The latter encompasses the former but is very different from it and it involves a much larger canvas of policy.

That said, it is worth reflecting on the concept of cyber security. It has at least eight “ingredients” or foundation elements, some of which are narrowly technical (but which all

⁵ See CCDCOE website: <https://ccdcoe.org/cyber-definitions.html>.

⁶ Thomas Rid, *Cyber War Will Not Take Place*, Hurst: London 2013.

involve human input and institutions) and others which are simultaneously technical and deeply dependent on the character of the non-technical ecosystem. One view of these ingredients is captured in the graphic below (Figure 2) which describes them as vectors of attack and response, each of which can involve civil or military targets or actions.

FIGURE 2: A CYBER SECURITY MODEL⁷

Eight Vectors of Attack and Response*

Cyber security must address a range of political, social, legal, technical, management and personnel issues.

*Source: adapted from a Bell Labs graphic



The meaning of each of the terms describing a vector is self-evident, but “ecosystem” is worthy of calling as we consider a national security environment. The ecosystem for military purposes must be understood to include the entire “infosphere”, including attack and defence systems of potential or actual enemies and allies. This approach leads us toward cyber impacts on warfare and war planning beyond those involving traditional notions of “cyber security” (involving computer software and hardware).

But this approach does not go far enough. It is a framework developed by engineers to address problems of protection of information and information systems largely at the enterprise or network level and in peace time. Though the eight-ingredient framework is a useful departure point for broadening our understanding of what shapes security in cyber space in the military sphere, the framework does not do justice to wider political, economic, legal and social aspects of war fighting in the kinetic space. All military strategy and planning for any kind of war depend on the political, economic, legal and social environment as much as they do on engineering, systems management or capability-based approaches.

For this reason, we are obliged to understand the term “cyber war” (adapting Clausewitz) to refer to the continuation of politics through cyber means with warlike intent. Cyber means must involve “machine-based computation” with or without support from kinetic military capabilities (missiles, bombs, guns). But “cyber war” independent of the non-

⁷ Graphic adapted from a Bell labs graphic and designed by Kurt Barnett, UNSW Canberra.

cyber domain, is as Rid argues, probably unimaginable. This paper therefore see the interests of national defence planning as better served by using a concept like “cyber-enabled war”, since war of any kind is an act involving the political, economic and civilian resources of states, as well as their military technological resources. We must also note that most developed countries depend on computers and IT-based communications systems for the targeting and operation of all modern missiles, bombs and guns. One of the best scholarly analyses of the impact of the information age on war may be a 2009 paper by Amit Sharma.⁸ He addresses the strategic impact on war fighting goals of the information age in a way that few scholars have done, even in leading think tanks in the United States.

For this reason, among others, the use of the term “cyber-enabled war” in this paper should not be seen as conforming in definitional terms to the meaning either of the term “information operations” or the term “cyber space operations”, as used by the U.S. Joint Chiefs in their doctrinal publications,⁹ since these U.S. terms are intended only to convey the scope of military operations that do not by themselves constitute the totality of a state’s strategic objectives and actions in any war, including in “cyber-enabled war”. The U.S. government avoids public discussion of concepts like “cyber war”, even though, as is clear in later this paper, the current Administration assigns an overwhelming centrality in its military strategy to cyber space.

A unifying element between the concept of “cyber-enabled war” and “information operations”, is the concept of “information dominance” as the principal organising objective of national security policy (preparation for war) in the information era. Both the United States and China have used this concept but not always with the consistency one might expect.

In sum, the author does not see cyber space as a separate domain¹⁰ of military, social, economic or political life. It cuts across all domains. Cyberspace governs all economic, social, scientific, business and medical activity dependent on any sort of computerized record keeping or more complex analysis. In military affairs, cyber space encompasses the entire fabric of strategic command and control, weapons systems, battle space management and intelligence dissemination, on which national military security depends. Cyber space unifies all domains of warfare, especially its political control and its political impacts.

Moreover, the U.S. Joint Chiefs have identified three layers of policy and operational activity in cyberspace: physical, logical and the “persona”, but go further by integrating these into consideration of the environments (informational, operational and political), and considerations like the relationship between information operations and cyber space operations, and the involvement of the private sector.¹¹

⁸ Amit Sharma, “Cyber Wars: A Paradigm Shift from Means to End”, 2009, available at <https://ccdcoc.org/publications/books/VirtualBattlefield.pdf>.

⁹ U.S. Joint Chiefs of Staff (JCS), *Cyberspace Operations*, 2013, JP 3-12R, www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf; and U.S. Joint Chiefs of Staff, *Information Operations*, 2012, JP 3-13, www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

¹⁰ The choice by the United States government and its armed forces to refer to cyber space as a fifth domain is understandable from an organizational point of view. It was easier politically for the government to stand up its new Cyber Command as a separate command if it was presented as an add-on to the existing single services not taking over key parts of them. But it is important to note that language around “fifth domain” is politically loaded and organisationally driven, rather than a statement of reality. The U.S. decision to set up a national Cyber Command announced in mid-2009, was followed by formal establishment of cyber commands in the single services (air force in August 2009, marine corps in October 2009, navy in January 2010, army in October 2010). The USAF had been in lead with its efforts to set up a new cyber command beginning in 2006 but this was subsumed into the idea of setting up a unified command. The single service cyber commands now owe their loyalty as much to the joint Cyber Command and other unified commands as to the single services.

¹¹ See JCS, *Cyberspace Operations*, 2013, pp. 2-8.

International Trends in Planning for Cyber-enabled War

The national security needs of middle powers should be shaped above all by the threats or opportunities emanating from more powerful countries or non-state actors of military significance to them. This involves comprehension not only of their intent and capabilities of today but also of their likely intent and capabilities in the future. This section of the paper looks at two cases: China and the United States. Since national security is a balance between political, economic, military and social considerations, any estimate of how the two great powers impact the security needs of other countries in cyber space must address the full spectrum of national security: economic as well as military. The economic and social bases of national security include a country's national industry base, its scientific and technical potential, and the skills of its people. The political setting is also an essential determinant of war policy, so this section concludes with a review of the dominant trend in war policy globally: that of war avoidance in a situation of cyber arms racing.

Cyber Military Policy in China

China is a country of immense national security interest to most middle powers, not least because of its economic weight and its value as an economic partner. Chinese leaders accept the view that the cyber age is revolutionary in its impact. In February 2014, President Xi told his country and the world that the government would do everything needed for the country to become a cyber power.¹² As analysed in my book, *Cyber Policy in China*, this announcement came after almost 15 years after China first committed itself to the goal of what it called informatisation: the maximum exploitation of advanced information and communications technologies to all walks of life, including military power and internal security.¹³ The Xi announcement was intended by him to convey the view that China was lagging badly in cyber capability across a broad range of civil and military missions and interests and that it would henceforth work much harder to catch up.

Cyber Power Intent: In September 2014, Xi told the country it needed a new cyber military strategy. In December 2014, the government introduced new regulations for cyber security intended to help promote the rapid growth of China's domestic cyber security industry. In May 2015, the country issued a new Military Strategy in which the government declared for the first time in such a document the idea that "Outer space and cyber space have become new commanding heights in strategic competition among all parties".¹⁴

Since declaring his intent in February 2014 to do whatever was needed for China to become a cyber power, President Xi and his government have been hyperactive on all relevant fronts: political, legal, economic, organisational and diplomatic. Leadership attention to this set of issues became even more focused in May 2014 when the United States indicted

¹² Xinhua, "Xi Jinping Leads Internet Security Group", 27 February 2015, http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm.

¹³ Greg Austin, *Cyber Policy in China*, Cambridge UK: Polity Press, 2014.

¹⁴ China, Information Office of the State Council, "China's Military Strategy", May 2015, http://news.xinhuanet.com/english/china/2015-05/26/c_134271001.htm.

five Chinese military personnel for cyber espionage involving commercial secrets of U.S.-based corporations.¹⁵

Today, China is among the G20 countries with a very high level of government commitment to transform itself to exploit the information revolution. Most middle powers can learn from that level of commitment. In 2015, the World Economic Forum ranked China at 25th in the world in terms of the importance of ICTs in government vision of the future.¹⁶ Australia was at 40th, behind countries like Azerbaijan, The Gambia, Indonesia, Macedonia and New Zealand (ranked 7th). Japan, the Republic of Korea, and Malaysia were ranked ahead of China and Australia in terms of government commitment to “network readiness” and preparation for the information age. India was ranked at 71st on this criterion.

Cyber S&T: The scale of the China’s ambition to become a world leader in the S&T base of cyber power is documented in a 2011 plan by the country’s Academy of Sciences, called *Information Science and Technology in China: A Roadmap to 2050*. The vision is staggeringly ambitious and complex. It sees China approaching the frontiers of science, economics and social organization in the sphere of information technology by mid-century.

One impetus for the 2011 report was a strategy document, *Technological Revolution and China's Future: Innovation 2050*, from the Academy of Sciences which served not just as an overarching mobilizing document, but also marked the launch of a series of seventeen subsequent sector-based roadmap reports also looking ahead to 2050. The 2009 foundation report on innovation, which had involved some 300 Academy researchers and experts for more than a year, recommended that China prepare itself for a new revolution in S&T in the coming ten to twenty years in green energy, artificial intelligence, sustainable development, information networking systems, environmental preservation, space and ocean systems, and, most interestingly, national security and public security systems.

This all means that China as an economic and military actor in cyber space is determined to look and feel very different in 20 years time. For the benchmarking exercise in this current paper, we need therefore to ask how in the next 20 years will China change its S&T profile in cyber space and how middle powers can benefit from that or otherwise secure their national security interests in respect of China? This benchmarking leads not just to an academic comparison of estimated static national capability at given intervals, but also provides an insight into a dynamic policy process inside China in which other countries may seek to intervene to shape China’s choices to meet its strategic interests. This has diverse aspects, not least in respect of shaping normative behaviour about cyber war but also in respect of mutually advantageous development of both internationalised and exclusively sovereign S&T capability in both countries.

On current indications, within 20 years, China’s civil economic and military capabilities in cyber space will likely be very far ahead of most countries. A “great leap forward” by China in cyber war S&T relative to middle powers is inevitable given China’s current wealth and scientific and industrial capability. These other countries cannot do much about that. But they must prepare now to respond to the likely impact over the longer term of Beijing’s higher commitment in the past fifteen years to transformation through military cyber S&T compared with their own lack of commitment in key areas of policy over the same period.

¹⁵ For an extended discussion of this topic, see Greg Austin, “China’s Cyber Espionage: The National Security Dimension and U.S. Diplomacy” Discussion paper, 2015, available at http://thediplomat.com/wp-content/uploads/2015/05/thediplomat_2015-05-21_22-14-05.pdf.

¹⁶ See country profiles in World Economic Forum, *Global Information Technology Report 2015*, New York: Oxford University Press, for the World Economic Forum and others. Available at: http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf.

China's Concept of Distributed Warfare: In spite of undoubted successes in cyber espionage by the People's Liberation Army (PLA), China has moved quite slowly to adjust to the opportunities and challenges presented by cyber warfare.¹⁷ As mentioned above, it has made a series of new commitments and taken innovative measures to make the transition more quickly. Among these measures has been a move to joint or unified commands on the model of the U.S. armed forces. This has been based on the strong conviction of Chinese specialists, learning from their American counterparts, that maximum exploitation of and defence against cyber assets can only be assured through inter-service operations and advanced command control systems, which in turn are integrated with space-based surveillance, intelligence and targeting capability (C4ISTAR).¹⁸ It will take China a decade or two to bed down this transition.

Against the background of this perceived need to centralise command and control, and given China's past practices of clinging to outmoded patterns of national level command and control, including compartmented intelligence collection, it is all the more remarkable that it has in 2015 also committed to a countervailing doctrine that accepts the unique characteristic of cyber war called "distributed warfare". This is discussed later in the paper as a general phenomenon of high importance to any advanced country, but its application in the Chinese case is worth calling out. This is the principle that the operational combat environment of cyber-enabled war provides new opportunities for lower level formations widely dispersed to achieve strategic impacts in quite distant theatres. It also captures the consideration that the cyber environment places a premium on decapitation of superior level command authorities and even of basic communications systems in such a way that lower level combat units may need to fight without the benefit of continuous communications and intelligence feeds.

For China, recognition of this concept at the same time as it is moving towards centralisation is all the more remarkable. It has been captured in a turn of phrase in the 2015 military strategy: "you fight your way, I fight my way" in Section 3, "Guidelines of Active Defence": "the armed forces will adhere to the principles of flexibility, mobility and self-dependence so that 'you fight your way and I fight my way'. Integrated combat forces will be employed to prevail in system-vs-system operations featuring information dominance, precision strikes and joint operations."¹⁹ The two sentences presented together make plain the need for self-dependence even in operations intended to achieve information dominance.

In practical terms, it will take some five to ten years for China to develop its forces to any meaningful capability in this direction, but when it does achieve such a capability it will be at a scale that dwarfs that of smaller or less wealthy countries.

One practical implication of the shift in Chinese doctrine might be that any country operating with or against Chinese forces may well face isolated warships or ground force units acting confidently but with superseded orders and/or degraded intelligence assets because they have been cut off from superior echelons. This circumstance would not be desirable in fast-moving combat regardless of whether one is fighting with or against China.

Militia: China has two levels of reserve forces: what might be called normal reserve forces (reasonably well trained personnel and units that can be mobilised for combat anywhere in the service of the country; and far less-trained militia units which are normally assigned to civil defence tasks in their own locality. China has been developing cyber military capabilities in some militia units. While this might be construed as related to civil defence tasks in the home province, such as protection of cyber aspects of critical

¹⁷ This is discussed at length in Austin, *Cyber Policy in China*, Chapter 5.

¹⁸ C4ISTAR is a U.S. military acronym standing for "command, control, communications, computers, intelligence, surveillance, target acquisition, reconnaissance".

¹⁹ See http://www.chinadaily.com.cn/china/2015-05/26/content_20820628_3.htm.

infrastructure, the character of cyber war is far different from kinetic warfare in that the latter has always been shaped by geographic proximity to one degree or another. Since this civil defence function of militia has been revived and professionalised by Chinese leaders in the past decade and since the Chinese government has developed a massive internal surveillance and communications take-down capability based on cyber assets, China is exceptionally well placed to develop the most powerful and best-organized cyber militias in the world. It does not now have such a strong capability but it has taken steps along this path.

One added reason for China to develop cyber militia for integration into strategic and operational military tasks in wartime or in preparation for war is that it can draw on a massive pool of personnel in the civil work force who have high skills in their normal employment, in contrast to the PLA and reserve forces which will probably not have large numbers with the necessary skills on a scale that can compete with the U.S. forces for several decades. In the 10 to 20 year time frame, China's capability in cyber war will need to be assessed against the certain availability of a skilled workforce that no Western country could easily marshal in support of state policy short of an all-out declaration of war and general mobilisation.

Middle powers with a small highly trained cyber work force in uniform can usefully learn from the Chinese conditions that could, in a ten to fifteen year time frame, create a unique and powerful cyber militia capability.

Cyber Military Policy in the United States

Prompt Information Dominance: The United States, has a military strategy premised on information dominance as the foundation for what it calls "prompt global strike". This is a strategic objective in war, not just a tactical or theatre-level ambition. In conformity with this strategy, the United States is investing heavily in military uses of cyberspace and undertaking a rapid transformation of its forces. In 2015, the Pentagon issued a new Cyber Strategy²⁰ and the Commander of Cyber Command, Mike Rogers, issued a new planning document, titled "Beyond the Build".²¹

In U.S. planning, "cyber effect operations" in wartime seek to impair the confidentiality, integrity or availability of not just the machines but the data contained therein. This can include penetrating enemy intelligence systems and altering the information about one's own forces or even information about the disposition of the opposing country's forces. A Presidential Directive says that the United States will seek to apply "cyber effect operations" (COE) in all spheres of national activity affecting war, diplomacy and law enforcement.²² It says that offensive COE (OCO) "can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging". A Pentagon Law of War Manual issued in June 2015 says it is lawful for a country in wartime to undertake pre-emplacement of "logic bombs" in an enemy country's networks and information systems.²³

²⁰ United States. Department of Defense. "DoD Cyber Strategy", Washington DC, 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

²¹ U.S. Cyber Command, "Beyond the Build: Delivering Outcomes through Cyberspace", U.S. Department of Defence, Washington DC, June 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf.

²² United States. The White House. "Presidential Policy Directive 20: U.S. Cyber Operations Policy", 2012, available at: <http://fas.org/irp/offdocs/ppd/ppd-20.pdf>.

²³ United States. Department of Defense. *Department of Defense Law of War Manual*, Washington DC, 2015, p.995, <http://www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf>. The chapter on cyber operations specifically allows for pre-emplacement in wartime of cyber weapons (often called time-release

But there is a deeper dimension to the U.S. concept of cyber war beyond “information operations” or “cyber effect operations”. It relates to the role of information and how a country’s military power and strategic impact in war can be magnified by cyber means. In November 2012, the U.S. Joint Chiefs of Staff issued a new joint training manual on “Information operations”.²⁴ It identified the information environment as the aggregate of “individuals, organisations, and systems that collect, process, disseminate or act on information”. This is a strategic level orientation in which the United States aims above all else to disrupt the enemy’s decision-making as a prelude to and adjunct for kinetic operations: the integrated employment during military operations of information capabilities “in concert with other lines of operation, to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.” Cyber space operations, covered in part by a separate military doctrine (Joint Publication) under that rubric, provide a sub-component to information warfare strategy.²⁵

There are significant innovations in the 2015 policy statements from the Pentagon, including recognition in “Beyond the Build” that cyber defences in DoD are weaker than the threats it faces and that military units must be able to operate with degraded systems and a lack of cyber situational awareness (including command and control, intelligence and targeting data).

The most important lesson from the 2015 “DoD Cyber Strategy” is that to be effective in cyber-enabled war a country needs to plan for it, structure its forces accordingly, train them for it and develop the foundations for public engagement in it. The strategy document makes plain that there are so many foundations of cyber war that need to be out in the open, ranging from critical infrastructure protection to industry-based R&D and developing a civilian cyber work force. The document makes plain that any country intent on fighting a cyber capable adversary will be more effective the more it can talk publicly about the detail.

By comparison, there has been no little recognition among middle powers of the novel, arguably central role, of cyber-enabled warfare. There has also been no recognition of the value of public engagement in devising cyber war policies. Of some note, for example, as of 12 January 2016, the term “cyber effect” does not appear to be found anywhere on the Australian Department of Defence website, except in a submission for the Defence White paper by this author. It is more than likely that the concept is well known in development work in the ADF and that the ADF has already conducted cyber effect operations of some kind.²⁶ On the UK Ministry of Defence website there is not a similar aversion to the term, though one finds quickly a plea on 24 September 2015 by the current Secretary for Defence in the UK, Michael Fallon, to “put cyber front and centre of our thinking”.²⁷

Cyber Weapons for All: In spite of billions of dollars spent, new forces and command entities raised, and military education and recruitment revamped, the United States has in 2015 recognized how far it has yet to travel. On 3 June, the Commander of U.S. Cyber Command, Admiral Mike Rogers, observed as follows: “Our task is to make this domain

“logic bombs”): “Cyber operations can be a form of advance force operations, which precede the main effort in an objective area in order to prepare the objective for the main assault. For example, cyber operations may include reconnaissance (e.g., mapping a network), seizure of supporting positions (e.g., securing access to key network systems or nodes), and pre-emplacement of capabilities or weapons (e.g., implanting cyber access tools or malicious code).” While this statement in the manual refers to the U.S. view of its own actions in wartime, it would also be regarded by most states as the applicable international law in peacetime.

²⁴ JCS. “Information Operations”.

²⁵ JCS. “Cyberspace Operations”.

²⁶ This can be deduced from the public references to deployment of Defence civilian cyber specialists to combat areas in Afghanistan.

²⁷ Michael Fallon MP, Speech to Cyber Symposium 2015, Paris, 24 September 2015, <https://www.gov.uk/government/speeches/cyber-symposium-2015>.

understood by other warfighters and integrated into broader military and governmental operations while providing decisionmakers and operational commanders with a wider range of options while resources are constrained and threats are growing”.²⁸ In this short report, titled “Beyond the Build: Delivering Outcomes through Cyberspace”, Adm. Rogers emphasized the need to be able to offer commanders and policy makers “cyber tools in all phases of operations” and an increase in momentum in building both “capacity and capability”. One report of a large project on U.S. decision-making for information operations found that the DoD does not yet understand how to measure the decision-making agility of a cyberspace operations organization”.²⁹ These concepts rarely receive a public airing in the debates of middle powers.

R&D Innovation: One key element of U.S. national policy is its recognition of the need to “Leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation”.³⁰ It was expressed in just that language in the 2011 strategy which was the predecessor to the 2015 strategy.

In 2011, this was held up as one of the Department’s five principal strategies for cyberspace. The language was not picked up in the same way in the 2015 strategy which has a much sharper focus on operational aspects of the cyber war problem. Yet the centrality of the civil sector underpinning of the country’s cyber war capability is visible through the 2015 document. The references from the 2011 strategy provide a more concentrated expression of the set of issues involved in innovation policy for defence purposes, and these are highly relevant to middle powers. It makes the obvious commitment to catalysing new education opportunities in a situation of high and unmet demand: “catalyse U.S. scientific, academic, and economic resources to build a pool of talented civilian and military personnel to operate in cyberspace”. But it says that its plans in this area of skill development will be paradigm changing and will include the private sector:

- streamline hiring practices for its cyber workforce
- exchange programs to allow for “no penalty” cross-flow of cyber professionals between the public and private sectors to retain and grow innovative cyber talent
- adoption and scaling of cross-generational mentoring programs
- the development of Reserve and National Guard cyber capabilities
- infusing an entrepreneurial approach in cyber workforce development
- preserving and developing DoD’s intellectual capital
- replicate in the DoD the dynamism of the private sector
- harness the power of emerging computing concepts (especially speed and incremental development rather than a single deployment of large, complex systems)
- opportunities for small and medium-sized businesses and entrepreneurs to move concepts rapidly from innovative idea, to pilot program, to scaled adoption across the DoD enterprise
- emphasise agility, embrace new operating concepts, and foster collaboration across the scientific community.

Thus, for the United States, the national goal of ensuring military competitiveness in cyber space depends on a “paradigm changing” approach to innovation, national education and work force development, which will then be reflected in paradigm changing approaches

²⁸ Cyber Command, “Beyond the Build”.

²⁹ Steven W. Stone, “Factors Influencing Agility in Allocating Decision-Making Rights for Cyberspace Operations”, 20th ICCRTS Paper 096, June 2015, p. 1, <http://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/54da5be5e4b0e9d26e577151/14235965175/06/096.pdf>. Cited with the author’s permission.

³⁰ United States. Department of Defense. “Department of Defense Strategy for Operating in Cyberspace”, Washington DC, 2011, p. 11, available at: <http://www.defense.gov/news/d20110714cyber.pdf>.

to military workforce development and deployment. There is almost no evidence in the public domain that any middle power has such a comprehensive view of how to make this paradigm shift.

Military education: On a narrower military front, we can look at the education of junior officers and the role of their officer training academies in cyber policy development. The U.S. Military Academy at West Point is arguably the most advanced in all aspects. Here are some highlights:

- in 2001, it became the first undergraduate institution the National Security Agency certified as a “Center of Excellence” in Information Assurance Education
- in 2014, it ranked 9th among more than 5,000 tertiary education providers in the United States in terms of quality of education in cyber security
- a Cadet Cyber Enrichment Program offering internships in industry
- a Cyber Leaders Development Program providing up to 800 hours non-academic training for each cadet
- a community outreach program where cadets teach local students cyber security
- an Army Cyber Institute (cyber warfare research and teaching, set up in 2014; planned for 75 staff by 2017, funded in excess of \$20 million) which involves cadets in its work
- Co-publisher of the journal *Cyber Defense Review* (launched February 2015)
- Cyber Research Centre (in the Electrical Engineering and Computer Science Faculty)
- Host of the first Joint Service Academy Cyber Security Summit in May 2015.

The United States Air Force Academy (USAFA) has extensive cadet-based programs in cyber security, outer space operations and broader challenges of technological and management innovation. Its Center of Innovation combines a range of disciplines pertinent to the broader information revolution in civil affairs or the revolution in military affairs.³¹ The U.S. Naval Academy has an undergraduate major in Cyber Operations.

War Avoidance and Peace Building

At the start of this section of the paper, I noted that the national security needs of middle powers in cyber space should be shaped in large part by the military intent and capabilities of other actors. But these needs must also be driven, above all else, by the goal of war avoidance, Diplomacy and politics are the main tools in war avoidance. Therefore the trend in global politics toward or away from confrontation in cyber space or on cyberspace issues should be a major driver of national security planning for middle powers. The global trend on this front is mixed, with both increasing tensions and stepped-up efforts to reduce tensions. The seriousness of this consideration should not be under-estimated.

The importance can be illustrated at one extreme end of the spectrum by developments involving the nuclear forces of Russia and the United States.³² In June 2013, Russia and the United States agreed to set up a cyber-risk reduction center (a hot line) staffed by technical specialists inside the existing bilateral nuclear risk reduction center. Its purpose is to allow the two countries to exchange information on cyber incidents that might impinge

³¹ See the center’s website <http://www.usafa.edu/df/dfe/dfer/centers/coi/>.

³² For an extended analysis, see Greg Austin and Pavel Sharikov, “Preemption is Victory: Aggravated Nuclear Instability of the Information Age”, Working Paper, January 2015.

on nuclear military readiness. This was an important development in the bilateral cyber military relationship.³³

Yet in December 2014, Russia's revised military doctrine declared that the U.S. cyber-enabled strategy of "Prompt Global Strike" is one of Russia's four main military dangers.³⁴ The Russian government had been a little more circumspect in its 2010 doctrine with the statement that the only military nuclear threat it faced was "disruption of the functioning of its [Russia's] strategic nuclear forces, its systems of missile warning and control in outer space or of nuclear munitions storage facilities".³⁵ By October 2014, Russia had already acted on its increased concern about cyber threats, including through the deployment into its strategic missile forces of cyber defence units for the first time.³⁶ This link between cyber risk reduction and nuclear threats goes a long way to explaining rhetoric like a "cyber Pearl Harbor" used by former CIA Director Leon Panetta in October 2012.

The case of United States/China relations on military uses of cyber space is also very important in terms of overall strategic stability. According to the few authoritative sources available, China's military leaders are deeply disturbed by U.S. policy and see it as new evidence of muscle-flexing and dominating behaviour.³⁷ This concern is aggravated by perceptions of inadequacy in cyber warfare capabilities relative to the United States, and a sense in China of profound weakness in the face of the information and electronic warfare power of the Americans' global alliances. The core diplomatic challenge is how to manage the asymmetry in cyber military power (which will persist for some time) without falling into a new Cold War.³⁸

At the other end of the spectrum of cyber space interaction among states are a string of cooperative measures over more than decade in multilateral and bilateral settings. These include agreements in the G20, APEC, the ASEAN Regional Forum and various iterations of a Group of Governmental Experts (GGE) under the auspices of the United Nations looking at international security aspects of information and communications technology.³⁹ (The detail of the UN GGE report is discussed later in the paper.) By 2015, the overwhelming message of these initiatives was that global and national economic stability, as well as plain good

³³ For an extended discussion of the evolution of that relationship, see Franz Stefan Gady and Greg Austin, "Russia, the United States, and Cyber Diplomacy: Opening the Doors", EastWest Institute, New York/Brussels/Moscow, September 2010, http://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf.

³⁴ Russia. "Military Doctrine of the Russian Federation" (*Voennaya doktrina Russkoi Federatsii*), issued December 2014, <http://news.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf>.

³⁵ "The Military Doctrine of the Russian Federation", 5 February 2010, translation, Carnegie Endowment, http://carnegieendowment.org/files/2010russia_military_doctrine.pdf. This statement is also in its 2014 doctrine. See "Military Doctrine of the Russian Federation" 2014.

³⁶ RIA Novosti, "Russia Strategic Missile Forces Create Cybersecurity Units: Defense Ministry", 16 October 2014, <http://sputniknews.com/military/20141016/194157367/Russian-Strategic-Missile-Forces-Create-Cybersecurity-Units.html>.

³⁷ See Greg Austin, "Managing Asymmetries in Chinese and American Cyber Power", *Georgetown Journal of International Affairs*, "International Engagement on Cyber IV", October 2014, 141-151; and Austin, *Cyber Policy in China*.

³⁸ For an extended analysis of background to U.S./China relations on cyber space issues and policy recommendations, see Greg Austin, "China's Approach to International Legal Norms for Cyber Space", (in publication with the NATO Cyber Defence Centre of Excellence); and Greg Austin and Franz Gady, "Cyber Detente between the United States and China", EastWest Institute, New York/Brussels/Moscow, November 2012, <http://www.eastwest.ngo/idea/cyber-detente-between-united-states-and-china>.

³⁹ An extensive overview of these can be found in Greg Austin, Bruce McConnell, Eric Cappon, Nadya Kostyuk, "A Measure of Restraint in Cyberspace: Reducing Risk to Civil Nuclear Assets", EastWest Institute, 2014, pp. 13-14, <http://www.eastwest.ngo/sites/default/files/A%20Measure%20of%20Restraint%20in%20Cyberspace.pdf>.

governance, depend on constraining state-on-state cyber attacks in peacetime.⁴⁰ An equally important objective of these efforts has been to contain cyber probing and attacks in order to prevent unintended conflict escalation. The management of these issues was seen as a protracted but feasible process in an environment where all major powers not only see war amongst them as highly unlikely but also hold up this view as a major plank of policy.

The most surprising moves in 2015 were bilateral, between China and Russia and between China and the United States.

On 8 May, China and Russia concluded a formal agreement with Russia not to interfere unlawfully in each other's information resources and networks.⁴¹ (In January, China and Russia had participated in tabling a slightly revised draft of the proposed code of conduct for cyberspace initially submitted to the United Nations in 2011.)⁴²

By signing the new bilateral agreement in May, China and Russia together appear to have pre-empted the advisory effect of the 2015 GGE report, and its recent predecessors, to give legal effect to some of the principles proposed. The bilateral agreement also goes very close to constituting a formal military alliance in cyber space, since it lays out a mutual obligation of assistance in the event of a wide range of cyber attacks.

The Russia/China agreement is a fulfilment of a decade of involvement by the two countries in cooperative measures on cyber space governance, including through the Shanghai Cooperation Organization (SCO) talks beginning in 2006. The 2015 agreement formalizes at a bilateral level the intensifying multilateral effort building off the proposal in the UN system for a code of conduct in cyberspace. The agreement is as much about that effort as it is about strengthening each other in the face of US cyber pre-eminence. Article one describes malicious use of cyber space "as a fundamental threat to international security". Article 4 commits the two countries not to undertake actions like "unlawful use or unsanctioned interference in the information resources of the other side, particularly through computer attack".

This is not a commitment to refrain from all use of military cyber assets against each other. Neither Russia nor China regards cyber espionage or preparations for war in cyberspace as "unlawful" or "unsanctioned". Of some note, Article 6.2 commits both parties to protect state secrets of the other, and references a prior bilateral treaty with that precise effect dating from 24 May 2000.

In early September 2015, in advance of a state visit by President Xi Jinping to the United States, China sent the Politburo member with responsibility for its non-military spy agencies, Meng Jianzhu,⁴³ to Washington for several days of official discussions to try to

⁴⁰ Progress in 2015 has been summarized in Greg Austin, Bruce McConnell and Jan Neutze, "Promoting International Cyber Norms: A New Advocacy Forum", EastWest Institute, New York, December 2015, <http://www2.ewi.info/idea/slowing-cyber-arms-race>.

⁴¹ For a text of the approved agreement, see Russia. Federal Government. Order on the Signing on an Agreement between the Russian Federation and the People's Republic of China on Cooperation in the Field of Securing International Information Security, (in Russian), Moscow, 30 April 2015, <http://pravo.gov.ru/laws/acts/34/555656451088.html>.

⁴² See United Nations, Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/69/723, 13 January 2015, <https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf>.

⁴³ Of special note, Meng controls the civilian spy agencies (Ministry of State Security for external intelligence and Ministry of Public Security for domestic intelligence). He does not control the main signals intelligence agency of China which sits in the People's Liberation Army, under the control of the Central Military Commission of the Chinese Communist Party (CCP). Meng is the Secretary of the Central Political and Legal Commission of the CCP, one of the most powerful political bodies in the country because of its role is the protection of all aspects of the "political and legal" system in the country.

dampen controversies within the United States about the norms of cyber espionage.⁴⁴ This was at that time the high point in direct official contact on the subject resulting from a robust diplomatic campaign by the United States which reached a new peak in March 2013 when National Security Adviser Thomas Donilon made public demands on China to abide by rules of the road prohibiting cyber espionage for commercial purposes.⁴⁵

The Meng visit was highly productive, with the two countries agreeing not to conduct commercial espionage against each other for the benefit of their own companies and to set up a Cabinet-level working group for problem solving on cyber security issues from a law enforcement angle.⁴⁶

Just weeks earlier, the United Nations published the report of the fourth GGE.⁴⁷ With Chinese representation in the group, this report marked a new peak in intergovernmental consensus on some related issues, including most importantly the endorsement of a range of possible “voluntary, non-binding norms, rules or principles” for restraint in international cyber practices.

The 2015 GGE report proposed three potential “voluntary non-binding norms” for state behavior in cyber space:

- states should not attack each other’s critical infrastructure for the purpose of damaging it
- states should not target each other’s cyber emergency response systems
- states should assist in the investigation of cyberattacks and cybercrime launched from their territories when requested to do so by other states.⁴⁸

As promising as these moves in the direction of restraint and war avoidance have been, they only begin to scratch the surface of what is needed. There is no commitment among the major military powers of the world to any idea of military sufficiency in cyber space or the idea of the security dilemma (the concept that when a state strengthens its own military power such action can have the unintended effect of weakening its security because it prompts military rivals to increase their capabilities).

Cyber War: Trends and Technologies

In 2009, Martin Libicki, one of the most respected scholars of cyber warfare, concluded in a report he wrote for the United States Air Force that “strategic cyberwar is unlikely to be decisive” and that “operational cyberwar has an important niche role but only that”.⁴⁹ In 2012, Thomas Rid and Peter McBurney from King’s College London made an important distinction between target-specific cyber weapons that may be high value in terms of effect and those of more general application (not target-specific) that are of lower value in

⁴⁴ White House, “Readout of Senior Administration Officials’ Meeting with Secretary of the Central Political and Legal Affairs Commission of the Communist Party of China Meng Jianzhu”, 12 September 2015, <https://www.whitehouse.gov/the-press-office/2015/09/12/readout-senior-administration-officials-meeting-secretary-central>.

⁴⁵ Greg Austin, “Cybersecurity: The Toughest Diplomatic Challenge Is China’s Weakness”, The Global Journal, April 2, 2013, <http://theglobaljournal.net/article/view/1049/>.

⁴⁶ For further analysis of the agreements, see Greg Austin, “Why the China-US Cyber Agreement May Prove Destructive”, The Diplomat, 7 October 2015, <http://thediplomat.com/2015/10/why-the-china-us-cyber-agreement-may-prove-destructive/>.

⁴⁷ United Nations, “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security” (UN GGE 2015), A/70/174, 22 July 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

⁴⁸ UN, GGE 2015.

⁴⁹ Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica CA: Rand Corporation, 2015.

terms of effect.⁵⁰ They say there is a clear penalty involved in developing the high-value weapons which “increase the resources, intelligence and time required for development and deployment” and are “likely to decrease the number of targets” and the “political utility of cyber-weapons”.

These assessments are sound, but they must be interpreted against the definitions of “cyber war” or “cyber weapon” that the authors use. In the Libicki case, his definition of cyber war was a narrow one (does not involve “real” war, that is a physical one),⁵¹ and Rid and McBurney define a cyber weapon as “computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings.”⁵²

There are at least three important dimensions of the policy problem presented by cyber-enabled war that such assessments do not take into account:

- will the cost/benefit relationship in technical development and use of cyber weapons change in the 10-20 year time frame?
- will the political character of a cyber weapon change as countries accumulate entire cyber arsenals, rather than single cyber weapons?
- does the political character of a cyber weapon change as countries move away from conventional military strategies to information age strategies where information dominance is judged to be the decisive capability?

My answer to all three questions would be yes. Over time, the conclusions by Libicki, Rid and McBurney are likely to be less relevant. For the purposes of this paper, we must note the highly dynamic character of the policy field represented by cyber-enabled war as countries accumulate capability, as technological options expand, and as key governments of interest continue to move decisively toward information dominance as an over-arching military strategy.

One of the best descriptions of the trends may be a 2011 book, *America the Vulnerable*, by the former Inspector General of the U.S. National Security Agency, Joel Brenner, who takes a distinctly non-technical approach and accords political and economic underpinnings of war and strategy a higher place than most specialists on cyber war.⁵³ While not agreeing with a number of his conclusions, I would like to illustrate the preceding point by calling out his understanding of how China has reacted to U.S. and Allied capability for information operations over the time since the first Gulf War in 1991 with a deepening and quickening attention to cyber warfare.⁵⁴ This is laid out in different parts of the book, and is essential for understanding that the technologies and strategies of cyber-enabled warfare are not static—anything but! One essential take away from the Brenner book is that cyber war as a real-life phenomenon (budgets, soldiers, politicians, industry and war-fighting) is only in its infancy and that it may be about to mature very quickly.

A second essential conclusion from the Brenner book is a very stark one that has grave national security implications for war planning by middle powers. Brenner concludes that his country “cannot defend our [its] electronic networks that control our energy supply, keep aircraft from colliding in midair, clear financial transactions, or make it possible for the President to communicate with his cabinet secretaries”.⁵⁵ For any country, as cyber war

⁵⁰ Thomas Rid and Peter McBurney, “Cyber Weapons”, *RUSI Journal*, February/March 2012, vol. 157, no. 1 pp. 6–13, 6, https://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf.

⁵¹ In his chapter six, Libicki looks at the relationship between the two forms of war.

⁵² Rid and McBurney, p. 7.

⁵³ Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime and Warfare*, New York: Penguin Press, 2011.

⁵⁴ Brenner, *America the Vulnerable*, 117-9, 121-2, 125-7, 130-1, 131-36, 137-47, 153-4.

⁵⁵ Brenner, *America the Vulnerable*, p.245.

capabilities of potential adversaries expand, those highly vulnerable aspects of cyber civil infrastructure that underpin military preparedness, including mobilization of forces through civil airspace, also become more likely targets.

Brenner aptly titles his first chapter, “Electronically Undressed”. If the United States cannot defend its critical infrastructure in cyber space at present, and it cannot, and if the world is on the edge of a rapid expansion of cyber warfare capabilities by the most powerful countries, this would appear to have implications which middle power should publicly acknowledge and to which they should more consistently provide appropriate responses.

Brenner outlines a suite of policy measures, most of which are highly reasonable. While few address issues of war fighting capability or strategy, all of them represent potential contributions to national security preparedness in cyber space. For example, he calls out the need to move toward highly secure computing (“verifiable software and firmware”) by promoting public support for research in this area. The implications of this transition are spelled out at length in a 2014 paper from the EastWest Institute, which argued that governments have tolerated for too long the exposure of their security to vulnerabilities of the sort outlined by Brenner.⁵⁶ This EastWest paper called on governments to “send clear [market] signals to enable security-driven IT innovation, starting top-down with the highest security requirements in the highest value targets”. As importantly, it urged governments to “cooperate internationally to realize this new paradigm quickly and to stem the evolution of high-end cyber attackers before they can inflict more damage”.

The Brenner book is but one of many sources indicating the scale of the challenge in national security arising from the rapidly intensifying transformations of the information age. A policy framework that is slow, incremental and largely oblivious to the emerging trends of cyber war (the sort of framework most middle powers have had) will fail badly. For this reason, the September 2015 document, “Beyond the Build”, issued by the Commander of U.S. Cyber Command, Adm. Rogers, and referred to above, must stand as a summary indicator of where all countries seeking to maximize national security and cyber war planning must head in the 10-20 year time frame.

We might note two U.S. assessments, one official and one from an academic source:

- *U.S. Worldwide Threat assessment 2015*: “2014 saw, for the first time, destructive cyber attacks carried out on US soil by nation state entities” “we must be prepared for a catastrophic large scale strike – a so-called cyber Armageddon” ... “unpredictable instability is the new normal”⁵⁷
- Georgia Tech: *Emerging Cyber Threats Report 2015*: “Low-intensity online nation-state conflicts become the rule, not the exception”⁵⁸

⁵⁶ Sandro Gaycken and Greg Austin, “Resetting the System: Why Highly Secure Computing Should Be the Priority of Cybersecurity Policies”, EastWest Institute, New York/Brussels/Moscow, January 2014, p.5, <http://www.eastwest.ngo/sites/default/files/Resetting%20the%20System.pdf>.

⁵⁷ Director of National Intelligence, Remarks as delivered by The Honorable James R. Clapper, Director of National Intelligence, Opening Statement to the Worldwide Threat Assessment Hearing, Senate Armed Services Committee, Thursday, Feb. 26, 2015, <http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee>. The Clapper statement on cyber Armageddon was prefaced with the word “though”, and he contrasted that future planning need with the current reality of a “constant and expanding barrage of cyberattacks for some time”. He did this to highlight the seriousness of the latter, not to suggest that the cyber Armageddon was not a focal point of U.S. planning from a defensive point of view. Clapper also said that the United States was still trying to decide how aggressive it should be in launching counter-attacks in cyber space, but this can only have been a reference to peacetime rather than open hostilities.

⁵⁸ Georgia Tech information Security Centre and the Georgia Tech Research Institute, “Emerging Cyber Threats Report 2015”, 2014, p. 13, https://www.gtisc.gatech.edu/pdf/Threats_Report_2015.pdf.

Special Features of Cyber War

Leaving aside the great powers preparations for cyber war for a moment, there are other important politico-strategic aspects of war in cyber space that have relevance regardless of the country involved and which are also likely to evolve in the next 10-20 years in ways that middle powers should take into account.

First, there is the new potential offered by cyber space for asymmetric warfare by weak military powers (and non-state actors) against states that are clearly superior in conventional (kinetic) military terms. While this concept has been present for a long time, it is not a static phenomenon but changes with advances in technology. According to a study, compiled by the U.S. Director of National Intelligence in 2000, of likely threats to 2015, asymmetric warfare was then the first of only three likely military threats faced by the United States.⁵⁹ The other two were strategic threats from weapons of mass destruction and regional conflict threats. The DNI report defined asymmetric conflicts as those in which “state and nonstate adversaries avoid direct engagements with the US military but devise strategies, tactics, and weapons—some improved by ‘sidewise’ technology—to minimize US strengths and exploit perceived weaknesses”. By 2015, the DNI confirmed in its annual worldwide threat assessment just this prognostication, though in slightly different words. Listing “cyber” first in its list of threats, DNI concluded: “the likelihood of a catastrophic attack from any particular actor is remote at this time”. He said that the more likely threat, rather than one that debilitates the entire US infrastructure, would be “an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security.”⁶⁰

Second, there is the opportunity for “distributed” warfare, a capability (and arguably a practice) that will become more pervasive over time. In simple terms, distributed warfare is the translation of the national-level use of coercive power to disconnected individual units, mirrors the same decentralisation of political authority that has been visible in the use of social media to break down the power of authoritarian regimes in places like Egypt or the Hong Kong Special Administrative Region. There are several ways of understanding this phenomenon in respect of military applications. One is to look at the role of patriotic hackers, whose potential in warfare may be likened to partisan forces capable of disrupting an enemy but which are either affiliated loosely with their home government or not connected at all, often acting against its interests or express wishes. Patriotic hacking is an important and evolving phenomenon in several regions, especially East Asia (most notably in China, South Korea and Japan).

Another dimension of distributed warfare is the contribution and role of cyber militias, people who have a civilian day job but who can be directed by the national government at short notice to participate in national security activities, including cyber war if need be. As noted above, China has an active program of developing cyber militia units, but also relies on its unique political system to co-opt companies and firms. The United States does not have such an explicit reliance on cyber militias, in part because it has an established network of high-tech companies who can be quickly and easily paid to feed into U.S. national security activities if need be. According to the government, it has at least 10,000 cleared

⁵⁹ Director of National Intelligence, “Global Trends 2015: A Dialogue about the Future with Non-Government Experts”, NIC2000-2, December 2000,

http://www.dni.gov/files/documents/Global%20Trends_2015%20Report.pdf.

⁶⁰ Director of National Intelligence, “Statement for the Record, Worldwide Cyber Threats, House Permanent Select Committee on Intelligence”, James R. Clapper, Director of National Intelligence, September 10, 2015, <http://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf>.

companies it can consult for advice on highly classified technical aspects of the country's intelligence needs.⁶¹

The above forms of distributed warfare are challenging enough to national security operations, demonstrated not least by the Snowden affair in which one of these paid employees was able to use his individual "network power" to blow open some of the most sensitive aspects of U.S. cyber warfare capability and preparations. The Snowden revelations on Operation Prism, which implicated nine leading U.S. corporations in direct and large scale involvement in U.S. national security missions in cyber space, produced an even more damaging outcome in that these companies reacted by distancing themselves from any political subordination to or co-optation by the national government as participants in distributed cyber warfare capability. Microsoft for example has made plain its position that it treats all clients equally, including the United States and China.⁶² This reverse positioning of U.S. corporations away from integration into the distributed warfare assets of the government was evident when U.S.-based company Symantec participated in the analysis of and revelations about Stuxnet, leading to the disruption of that live U.S. intelligence operation and subsequent exposure of it.⁶³ One implication of this is that middle powers must continually evaluate any presumption they make about the security affiliations and dispositions (patriotic or neutral) of foreign corporations, not to mention domestic ones.

But the biggest challenge presented by distributed warfare is the fundamental change in the relations between a central command authority and its deployed units. In an era of information dominance and concrete enemy plans for decapitation of command and control, whether through cyber or kinetic means, all military units must now have ways of re-connecting with each other if key links in the central chain are broken. As mentioned above, China has responded to this much more explicitly than most countries in its recent military strategy (May 2015). It foreshadows a lessening of central command authority to foster the conditions of victory in cyber war under the rubric of "self-dependence" for individual military units ("you fight your way and I fight my way").

One of the political consequences of distributed warfare and its asymmetric potential is that it may also break down the traditional value of military alliances, especially the provision of extended deterrence. Some countries benefit from the technical support of its intelligence alliances, especially the Five Eyes,⁶⁴ in preparing for cyber war and conducting information operations. Even in that case however, while U.K, Canadian, Australian and New Zealand forces enjoy considerable integration into advanced command and control arrangements with US. forces for operations, there is however considerable evidence to suggest that their reliance on the United State for extended deterrence may not have as much impact in cyber space as for kinetic operations. In NATO, the United States has agreed with its alliance partners that an attack in cyber space can constitute an armed attack for the purpose of invoking mutual response under Article 5 of the treaty. The question however is whether cyber incursions of a warlike character or preparatory to war would in practice attract that U.S. support. It is more than likely that middle powers allied to the United States would have to plan for a higher degree of self-reliance in cyber space than in maintaining

⁶¹ Director of National Intelligence, "Industry Snapshot: Summary of Partner Responses to the FY 2015-2019 IC S&T Investment Landscape," Washington DC, 2015, <http://www.dni.gov/files/documents/atf/In-STeP%20-%20Industry%20Snapshot.pdf>.

⁶² This has been made plain repeatedly by Microsoft representatives speaking at international conferences attended by the author.

⁶³ Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History", Wired Magazine, 7 November 2011, <http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/>.

⁶⁴ The "Five Eyes" is an intelligence alliance between the United States, the United Kingdom, Canada, New Zealand and Australia arising from their collaboration in the Second World War.

kinetic military capability because the recognition of thresholds of incursion or assault in cyber space is far less developed and far more ambiguous than in kinetic scenarios. There is little room for doubt about intent when several bomber aircraft of one country penetrate the airspace of another without prior clearance. This would constitute a threat of armed attack. The same clarity is not yet in place for cyber incursions.

Future Systems of Attack and Defence

Trends in technologies for cyber attack and defence have been described in many places: from government agencies, scholars, vendors, netizens and hackers. Those of significance for benchmarking national security needs range across all eight vectors of the “cyber flower” described above, but they also include those that cut across and combine the individual vectors. These might be called “systems of systems” technologies. The scale of the challenge in forecasting technologies of attack and defence systems should not be dumbed down by anyone person’s understanding of security in cyber space. The first thing that strikes a policy analyst coming to the question from a neutral, non-specialist position is the immense diversity of estimations about future technologies of attack and defence systems. There is also the consideration that novel (disruptive) cyber technologies will emerge and be deployable at short notice, in time periods as short as a matter of days in terms of warning.

From the point of view of benchmarking the national security needs of middle powers, this paper has chosen to highlight just a few ideas of future systems that are not particularly prominent in public discussion by officials or among specialists in middle powers.

If one looks narrowly at the typical security specialist’s horizon, the characterization of threat development around complex cyber attacks is a useful place to start. In 2015, a U.S. based analyst, Carl Herberger, the Vice President of Security Solutions at Radware, reported that in 2013 the average cyber attack he had observed involved seven attack vectors (though some had reached over 25 attack vectors), different phases (each with several waves), with successive phases relying on methods that worked in the previous phase but adding new attack vectors.⁶⁵ This was rather well captured in a FireEye presentation in 2013 which listed four characteristics of the emerging threat landscape: coordinated persistent threat actors, dynamic polymorphic malware, multi-vector attacks and multi-phase attacks.⁶⁶

These characterisations are very important benchmarks. But they don’t take us as far as we need to look. On the one hand, they address only a narrow slice of the eight vectors of attack, and don’t say a lot about defensive systems.

As one leading international example of future defensive systems, we might look at the topic of critical infrastructure protection and the acknowledged world leader in cyberspace defence of it, the Idaho National Laboratory (INL). The focus of this work is not military battlefield systems, but it provides many benchmarks for development of battlefield systems and for defence policy makers and military leaders who must be able to depend on certain critical infrastructure. After all, there is no victory in war without survivable critical infrastructure. That is one meaning of the word ‘critical’.

We can take the case of electric power supply which is just one of eight ingredients of cyber security. Not only is it controlled by digital assets, but it is possibly the most ignored vector of attack and response in cyber space. This was the subject of testimony of an Associate Director of INL, Mr Brent Stacey, on 21 October 2015, which is extracted verbatim below and which gives any country considerable cause for concern:

⁶⁵ See more at: <http://inspiratron.org/blog/2015/05/29/the-art-of-cyber-war/#sthash.LxJiSSic.dpuf>.

⁶⁶ See <http://www.exclusive-networks.be/wp-content/uploads/2013/11/FireEye-breakout-session.pdf>.

- The presumption that a control system is “air-gapped” is not an effective cyber security strategy. This has been demonstrated by over 600 assessments.
- Intrusion detection technology is not well developed for control system networks; the average length of time for detection of a malware intrusion is four months and typically identified by a third party.
- As the complexity and “interconnectedness” of control systems increase, the probability increases for unintended system failures of high consequence - independent of malicious intent.
- The dynamic threat is evolving faster than the cycle of measure and countermeasure, and far faster than the evolution of policy.
- The demand for trained cyber defenders with control systems knowledge vastly exceeds the supply.⁶⁷

The sort of defensive response outlined by INL is also quite instructive. It has identified a three tier approach rendered verbatim below:

1. Hygiene: “the foundation of our nation’s efforts , composed of the day - to-day measure and countermeasure battle”; “important routine tasks such as standards compliance, patching, and password management”; “primarily the role of industry, with both vendors and asset owners participating”.
2. Advanced persistent threat: “the more sophisticated criminal and nation state persistent campaigns”; requiring “a strategic partnership with industry and government”; “these roles are still evolving”; “ICS-CERT⁶⁸ provides critical surge response capacity and issues alerts of current vulnerabilities to the government and asset owners”
3. High impact low frequency events: “catastrophic and potentially cascading events that will likely require substantial time to assess, respond to, and recover from. This level is primarily the responsibility of the government.”

Research at INL focuses on the two highest priority tiers (#2 and #3 in the list above), aiming for a “two- to four-year research-to-deployment cycle” and to “achieve transformational innovations that improve the security of our power infrastructure by reducing complexity , implementing cyber-informed design, and integrating selected digital enhancements”. The laboratory “is pursuing a grand challenge to develop novel and deployable solutions to take a set of high value infrastructure assets off the table as targets”. This program assumes pervasive insecurity: It promotes “a paradigm shift in the methods used to historically develop control systems. This paradigm is predicated on the fact the traditional trust relationships in peer communications are no longer a satisfactory assumption. Instead, a resilient control system design expects a malicious actor or actions to be part of normal operation and is designed to mitigate such actions”.⁶⁹

Most middle powers have no comprehensive effort that remotely matches the approach adopted by INL, and in fact much of their governmental effort is spent on the

⁶⁷ United States. House of Representatives. Science Subcommittee on Energy And Science Subcommittee On Research And Technology, Written Testimony of Mr. Brent Stacey, Associate Laboratory Director for National & Homeland Security, Idaho National Laboratory, 21 October 2015, p.3, <http://docs.house.gov/meetings/SY/SY20/20151021/104072/HHRG-114-SY20-Wstate-StaceyB-20151021.pdf>.

⁶⁸ ICS-CERT is an acronym for “Industrial Control Systems Computer Emergency Response Team”.

⁶⁹ See website of Idaho National laboratory, https://inlportal.inl.gov/portal/server.pt/community/distinctive_signature_icis/315/grand_challenge.

lowest priority tier (#1 in the list above) identified by INL: the cyber security hygiene of operators and enterprises.

A 2012 UK analysis provides some additional insight into the processes threatening cyber resilience of another aspect of critical infrastructure, the financial services sector.⁷⁰ The study was based on consultation with industry. Interviewees identified as one of the top 3 technology risks the “development or emergence of new technology and poor change management in relation to new technologies”.⁷¹ A 2013 academic study on a similar subject warned against the danger of estimating risks in isolation from each other: “Estimation of CPS⁷² risks by naively aggregating risks due to reliability and security failures does not capture the externalities”.⁷³ It called out “biased security choices” that “reduce the effectiveness of security defenses”. Looking to future threats, it warned that CPS “are subjected to complex risks, of which very little is known despite the realization of their significance”.

Technologies of Decision-making

High performance computing, a technology that is well established though rapidly evolving, is being seen increasingly as an essential tool of cyber defence management at the national level military level, as well as a new weapon in the hands of adversaries. A 2014 paper from Sandia Laboratory lays out a future “technology of decision-making” based on high performance computing⁷⁴ that might usefully be understood by analogy as an attempt to create for cyberspace, as a global civil domain, an up-scaled version of the global strategic C4ISTAR system for U.S. command of its strategic nuclear weapons, including indicators and warning.

The study took as a core operating principle the proposition that the cyber security terrain for national decision-making is a “continuous lifecycle with human, organizational, legal, and technical interdependencies”. It identified seven high priority “wide-area problems” in the field of cyber security that have high relevance to middle powers in understanding its technologies of decision-making for cyber-enabled war. These priority problems, listed verbatim, are:

1. disjointed response to wide-area and multi-target attack
2. widely dispersed and fragmented detection and notification capabilities
3. ill-defined government, commercial, and academic roles and responsibilities
4. divided and rigid wide-area cyber protection posture
5. unresolved wide-area common and shared risks
6. fragile interdependent wide-area critical access and operations
7. unresolved attribution of attack and compromise.

⁷⁰ United Kingdom. Financial Conduct Authority, HM Treasury and the Bank of England, “Technology and Cyber Resilience Benchmarking Report 2012”, London 2013, <http://www.bankofengland.co.uk/financialstability/fsc/Documents/technologyandcyberresiliencebenchmarkingreport2012.pdf>

⁷¹ The other two were network and critical system outages, and access management and control of administration privileges.

⁷² Cloud Platform Services.

⁷³ Saurabh Amin, Galina A. Schwartz, Alefiya Hussain, “In Quest of Benchmarking Security Risks to Cyber-Physical Systems”, *IEEE Network*, January/February 2013, 19-24, 24, <http://www.eecs.berkeley.edu/~schwartz/IEEEMag2013.pdf>.

⁷⁴ Curtis M. Keliiaa and Jason R. Hamlet, “National Cyber Defense High Performance Computing and Analysis: Concepts, Planning and Roadmap”, SANDIA Report, SAND2010-4766, September 2010, pp.7-8, <http://prod.sandia.gov/techlib/access-control.cgi/2010/104766.pdf>.

The authors concluded by recommending areas for further research in high performance computing to support national security decision making for cyber space.⁷⁵

It is unsurprising that U.S. government laboratories have the remit and the resources to take on such challenges, and that scientists in middle powers do not have the same opportunities. As far as middle powers are concerned, in the absence of public disclosure about similar activities at the strategic level of warfare, we can probably conclude that the remit and resources for such analysis, and subsequent procurement action, are very different. Several middle powers do have well developed assets for research in and application of high performance computing, but in the absence of public evidence to this effect, one might conclude that these have not been rigorously applied to the special demands of decision-making for cyber-enabled war at the strategic level.

If we translate the ecosystem of threat and defence implied by the mere handful of trends in technology (and response to those trends) mentioned above, we can only conclude that middle powers are staring down the barrel of almost insurmountable challenges unless they are able to develop complex responsive systems of decision-making for medium intensity war that address simultaneous multi-vector, multi-front and multi-theatre attacks in cyber space by a determined enemy, including against civilian infrastructure and civilians involved in the war effort. And all of that before we even think about emerging technologies like quantum computing, anti-satellite weapons, mass deployment of drones as distributed airborne C4ISTAR platforms, a return to traditional HF-based communications for cyber activities, and laser-based communications.⁷⁶

Scenario Planning for Cyber-enabled War

There are many components to planning, funding and training a defence force for the future. One of the most important is the intelligence foundation: what are other countries doing and planning to do? What might they do in certain circumstances based on what we know? How might future technologies affect their military strategies? These are the sorts of issues canvassed above. An additional tool is that of scenario development, which is especially useful where uncertainty about the intelligence available will be high, as is certainly the case in cyber-enabled warfare. The value of scenario planning is widely appreciated in most military leaders, though not often exercised in respect of cyber-enabled warfare.

The merits of scenario planning as summarized by two research scholars for a NATO-related cyber conflict conference, are worthy of close scrutiny.⁷⁷ There are classic elements, such as the elucidation of likely geopolitical scenarios, but they also see merit in cyber-space scenarios for their ability to tease out alternative responses to future technologies and in creating a stimulus to change among policy makers and managers. They also call out, as Adm. Rogers has done, the value of providing a common ‘language’ and doctrinal approach to possible future trends in cyber war. Above all, the authors highly recommend the use of scenarios as a concrete tool for reducing strategic surprise (“Reduction of the impact of uncertainty through the notion of ‘robustness’”).

⁷⁵ These areas for research were: trusted connection and automated processes; informatics, statistics and anomalous behavior; mathematics analysis and intrusion detection; complexity science and emergent behavior; modeling and simulation; analysis and correlation algorithms; sociology and psychology.

⁷⁶ Robert Koch and Mario Golling, “Blackout and Now? Network Centric Warfare in an Anti-Access Area Denial Theatre”, in M. Maybaum, A.-M. Osula, and L. Lindström (eds), *2015 7th International Conference on Cyber Conflict: Architectures in Cyber Cyberspace*, Tallinn: NATO CCDCOE, 2015, 169-184, 178-180, https://ccdcoe.org/cycon/2015/proceedings/12_koch_golling.pdf.

⁷⁷ “The Use of Scenarios in Long Term Defence Planning”, April 2007, <https://plausiblefutures.wordpress.com/2007/04/10/the-use-of-scenarios-in-long-term-defence-planning/>.

Most middle powers have been involved in scenario planning for civil cyber emergencies. Few have published details of scenarios for cyber-enabled war, but there is no shortage of demonstration scenarios. As one example, in late 2014, the United States government conducted an exercise, Cyber Flag, with a wide number of scenario elements⁷⁸ that have not been present in similar public domain announcements in most middle powers about their preparation for cyber-enabled war. These included:

- joint force response to a regional crisis involving significant cyber military activity
- full spectrum military operations (with “cyber plus kinetic” combat goals)
- alliance cyber operations with air, land and naval forces
- operating while being subjected to cyberattacks affecting national command and control.

This type of exercise scenario is useful, but like most it has specific training and development purposes that need to be limited to the development stage of the forces involved in the exercise and do not necessarily reflect the totality of the type of situation (contingency) for which military planners at the executive level of government must prepare.

For the purposes of benchmarking international best practice in scenario development or contingency planning for cyber-enabled warfare, it would be important to undertake a detailed study since none seems to exist in the unclassified domain. But for the purposes of this paper, it may be sufficient to note that defence planning at the national level, in terms of future war, would be the “kingdom of the blind” if a country did not have an agreed vision of the likely contours of a cyber-enabled war. For the United States, one of the most cited for the United States is the case of a military confrontation with China over Taiwan.⁷⁹ This is highly credible and involves wide-ranging cyber attacks against U.S. civil infrastructure to prevent mobilisation of U.S. forces or delay their deployment to the Western Pacific.

An alternative way of constructing a scenario would be take the most notable incidents of state-sponsored and criminal cyber actions that might be most relevant to a particular type of medium intensity conflict and see how they might be combined to develop a scenario of relevance to particular countries. For a middle power, the list of possible attack vectors for cyber-enabled kinetic war would be long, but we can illustrate the scope by alluding to the following potential combination:

Estonia 2007 (a shut down of the financial and banking system) + China’s kinetic anti-satellite test 2007 + Stuxnet 2010 (cyber sabotage) + release by the group Anonymous of military personnel data + cutting of undersea cable (numerous incidents) + closing down of civil satellite links (Egypt) + closing down electric grids (U.S. operation in Yugoslavia 1999) + insertion of false data into military systems + attacks on Saudi Aramco + planting malware in civil aviation systems + opening flood gates on dams + closing down military communications.⁸⁰

Consideration of such scenarios leads us to only one of three possible conclusions about government policy in middle powers. First, medium intensity cyber-enabled war outlined in such a scenario may be such a remote possibility that we need not plan for it. Or, second, we have not studied it sufficiently to know or to have developed a national consensus

⁷⁸ Bill Gertz, “Cyber War Games Held”, *Washington Times*, 12 November 2014,

<http://www.washingtontimes.com/news/2014/nov/12/inside-the-ring-cyber-war-games-held/?page=all>.

⁷⁹ David C. Gompert and Martin Libicki, “Cyber Warfare and Sino-American Crisis Instability”, *Survival*, 56 (4), 7-22, <https://www.iiss.org/en/publications/survival/sections/2014-4667/survival--global-politics-and-strategy-august-september-2014-838b/56-4-02-gompert-and-libicki-04fc>.

⁸⁰ This sort of scenario was canvassed by Mark Seinor at an international conference on “Redefining R&D priorities for Australian Cyber Security” on 16 November 2015. See <https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/cyber-r-d> for a list of presentations, including that by Seinor.

on what type of cyber-enabled war we are most likely to face. Or third, we cannot regard cyber military policy in any country as mature until the government:

- has had an open and candid conversation in public with key stakeholders about the sort of threat scenarios our armed forces and communities may face in a medium intensity cyber-enabled war
- has developed defence policies and armed forces, supported by the civil sector, that could perform credibly in those scenarios given reasonable warning time
- has articulated a diplomatic strategy to reduce the risks of such a war if it looks like emerging
- has articulated a civil defence strategy for the inevitable high impact disruption of our civil economy and communities in such a war
- has set in place policies for development of our industry base and work force that can support all of the above to the extent that our national economy permits and limitations of alliance support dictate.

This author thinks that either the second or third possible conclusions are more logical than the first. I lean to the third, but am prepared to credit the second subject to much deeper analysis by relevant agencies, scholars and think tanks.

Conclusion and Recommendations

There are many departure points for benchmarking the national security needs of middle powers for cyber-enabled war. On the one hand, there are developing capabilities in countries like China and the United States, and middle powers therefore need to respond with their own sovereign capabilities. On the other hand, there is the important consideration that the technological trends in cyber warfare present a high complexity problem that defies past practices of defence policy formulation in most middle powers. The type of problem seems much bigger than the collectivity of institutions normally involved in framing national defence strategies for middle powers.

Just where a country needs to position itself in this highly dynamic and complex environment (the information ecosystem) is something that only the collective wisdom of its best and most expert minds, working in partnership, can answer. A prerequisite though has to be an open and public debate on the country's military, security and civil needs in cyber space and how well its emerging capabilities match those needs. Where this has begun to happen in a few middle powers (especially among members of the European Union and in Australia), the conclusion has been that the countries in question are badly lagging.

While a large slice of the national security cyber domain must remain secret, the public in any country and its key actors in policy (private sector companies, state governments, foreign suppliers, military allies, citizens, civil society groups, lawyers, judges, security agencies, university researchers and educators) need to see a clear vision, in a number of private places and in public, of where the government is headed. This vision needs to reconcile competing demands of national security in the information age with each other and with other public policy demands, such as open trade, international investment, privacy, industry regulation or industry support.

Based on this paper, governments and their armed forces leadership might consider articulating a comprehensive set of policies around the following benchmarks:

- A national innovation strategy that keeps the country at the forefront of international best practice in cyber technologies that can be applied in war

- A military strategy for cyber-enabled warfare that takes account of the proven and estimated character of such an armed conflict, including public intelligence assessments of likely cyber war threats and a top-end (but credible) scenario
- A strategy for sovereign cyber war capability and cyber survivability in a time of direct military confrontation with a major power
- A capital procurement program centred on advanced cyber-enabled war capabilities, including space-based assets and new technologies of decision-making
- A renovation of military institutions, training and education
- Necessary investments in niche technologies and research capabilities
- A strategy for managing civilian-military divides and critical infrastructure protection in times of military conflict
- A strategy for mobilizing cyber-capable reservists or civilians in times of military crisis
- A sharp distinction between the national needs for cyber security as largely a civil domain set of issues and the needs for cyber-enabled war fighting capability.

Above all else, a middle power needs to build a community of interest around the concept of cyber-enabled warfare with a recognised authoritative hub that can unite political, military, diplomatic, business, scientific and technical interests and expertise.

The famous war correspondent H.G. Wells observed in the 1930s that as military technology becomes more advanced, it becomes controlled by an increasingly small number of countries. One thing is crystal clear. Middle powers will not make the necessary transitions for cyber-enabled warfare at all unless they make a number of new policy commitments and substantial institutional transformations very soon.

At the same time, no middle power need stand alone in constructing a national defence strategy and diplomacy that can help secure the country's security interests in cyber space. This consideration has been driving work by the countries most passionately engaged in the UN GGE. If national defences in most countries are unlikely ever to rise to meet the potential threat of cyber-enabled warfare, the collective security response must remain a live and fruitful avenue for policy investment. There is ample evidence in this paper that the tension between advancing threats and multilateral restraint still favors the threats and not the defences. This is likely to remain the case as long as other developments (such as Russia's action in Crimea or a threat dynamic between China and the United States) reinforce geopolitical divides without compensating collective defence measures.

Cyber space, in spite of its military threat potential and high sensitivity for national security, may well be a locus for collective defence measures in the civil sector that can help to compensate for persistent or increasing geopolitical tensions either around military uses of cyber space or for other reasons. Such a conclusion is based in part on the symbiotic relationship between cyber space and national economic stability of even the most powerful military actors in cyber space. It is also based on evident commitment, for the most part, of all great and middle powers to war avoidance.

References

- Amin, Saurabh; Galina A. Schwartz, and Alefiya Hussain, “In Quest of Benchmarking Security Risks to Cyber-Physical Systems”, *IEEE Network*, January/February 2013, 19-24, 24, <http://www.eecs.berkeley.edu/~schwartz/IEEEMag2013.pdf>
- Austin, Greg, *Cyber Policy in China*, Cambridge UK: Polity Press, 2014
- ____ “International Legal Norms in Cyber Space: Evolution of China’s National Security Motivations”, forthcoming January 2016, with the NATO Cyber Defence Centre of Excellence as part of an edited volume on Cyber Norms
- ____ “China’s Security in the Information Age” in Lowell Dittmer and Yu Maochun (eds), *Routledge Handbook of Chinese Security*, Routledge, 2015, 355-370
- ____ “Australian Defence Policy in the Information Age”, Submission for the 2015 Australian Defence White Paper, 22 September 2014, 5,000 words, <http://www.defence.gov.au/Whitepaper/docs/028-Austin.pdf>
- ____ “Australia’s Digital Skills for Peace and War”, *Australian Journal of Telecommunications and the Digital Economy*, vol 2. No. 4, December 2014
- ____ “China’s Cyber Espionage: The National Security Dimension and U.S. Diplomacy” Discussion paper, 2015, available at http://thediplomat.com/wp-content/uploads/2015/05/thediplomat_2015-05-21_22-14-05.pdf
- ____ “Managing Asymmetries in Chinese and American Cyber Power”, *Georgetown Journal of International Affairs*, “International Engagement on Cyber IV”, October 2014, 141-151
- Austin, Greg (co-authored), Bruce McConnell and Jan Neutze, “Promoting International Cyber Norms: A New Advocacy Forum”, EastWest Institute, New York, December 2015, <http://www2.ewi.info/idea/slowing-cyber-arms-race>
- ____ and Franz Stefan Gady, “Cyber Detente between the United States and China”, EastWest Institute, New York/Brussels/Moscow, November 2012, <http://www.eastwest.ngo/idea/cyber-detente-between-united-states-and-china>
- ____ and Franz Stefan Gady, “Russia, the United States, and Cyber Diplomacy: Opening the Doors”, EastWest Institute, New York/Brussels/Moscow, September 2010, http://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf
- ____ and Pavel Sharikov, “Preemption is Victory: Aggravated Nuclear Instability of the Information Age”, co-authored with Pavel Sharikov (Moscow), Working Paper (unpublished), 2015
- ____ and Sandro Gaycken, “Resetting the System: Why Highly Secure Computing Should Be the Priority of Cybersecurity Policies”, EastWest Institute, New York/Brussels/Moscow, January 2014, <http://www.eastwest.ngo/sites/default/files/Resetting%20the%20System.pdf>
- ____ and Bruce McConnell, Eric Cappon, Nadya Kostyuk, “A Measure of Restraint in Cyberspace: Reducing Risk to Civil Nuclear Assets”, EastWest Institute, 2014
- Austin, Greg (news commentary) “Cybersecurity: The Toughest Diplomatic Challenge Is China’s Weakness”, *The Global Journal*, April 2, 2013, <http://theglobaljournal.net/article/view/1049/>
- ____ “Why the China-US Cyber Agreement May Prove Destructive”, *The Diplomat*, 7 October 2015, <http://thediplomat.com/2015/10/why-the-china-us-cyber-agreement-may-prove-destructive/>
- Brenner, Joel *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime and Warfare*, New York: Penguin Press, 2011.
- China. Information Office of the State Council. “China’s Military Strategy”, May 2015, http://news.xinhuanet.com/english/china/2015-05/26/c_134271001.htm

- Georgia Tech information Security Centre and the Georgia Tech Research Institute, “Emerging Cyber Threats Report 2015”, 2014, https://www.gtisc.gatech.edu/pdf/Threats_Report_2015.pdf
- Gompert, David C. and Martin Libicki, “Cyber Warfare and Sino-American Crisis Instability”, *Survival*, 56 (4), 7-22, <https://www.iiss.org/en/publications/survival/sections/2014-4667/survival--global-politics-and-strategy-august-september-2014-838b/56-4-02-gompert-and-libicki-04fc>
- Helgason, Sigurdur “International Benchmarking: Experiences from OECD Countries”, Paper Presented at a Conference Organised by the Danish Ministry of Finance on International Benchmarking, Copenhagen, 20-21 February 1997, p. 2, www.oecd.org/governance/budgeting/1902957.pdf
- Japan. 2013. “Cybersecurity Strategy: Towards a World-leading, Resilient and Vigorous Cyberspace”, Tokyo: Information Security Policy Council, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/JAP_NCSS2.pdf
- Kelliiaa, Curtis M. and Jason R. Hamlet, “National Cyber Defense High Performance Computing and Analysis: Concepts, Planning and Roadmap”, SANDIA Report, SAND2010-4766, September 2010
- Koch, Robert and Mario Golling, “Blackout and Now? Network Centric Warfare in an Anti-Access Area Denial Theatre”, in M. Maybaum, A.-M. Osula, and L. Lindström (eds), *2015 7th International Conference on Cyber Conflict: Architectures in Cyber Cyberspace*, Tallinn: NATO CCDCOE, 2015
- Libicki, Martin C. *Cyberdeterrence and Cyberwar*, Santa Monica CA: Rand Corporation, 2015
- Ormrod, David and Benjamin Turnbull, “Toward a Cyber Military Maturity Model”, abstract for a presentation at an international conference on Redefining R&D Priorities for Australian Cyber Security, 16 November 2015, University of New South Wales, Canberra, <https://www.unsw.adfa.edu.au/sites/accs/files/uploads/Military%20Cyber%20Maturity%20Model%20v1.pdf>
- Plausible Futures Newsletter, “The Use of Scenarios in Long Term Defence Planning”, April 2007, <https://plausiblefutures.wordpress.com/2007/04/10/the-use-of-scenarios-in-long-term-defence-planning/>
- Reuters. “China's Xi urges army to create strategy for information warfare”, 30 August 2014. Available at: <http://www.reuters.com/article/2014/08/30/us-china-xi-defence-idUSKBN0GU0H020140830>
- RIA Novosti, “Russia Strategic Missile Forces Create Cybersecurity Units: Defense Ministry”, 16 October 2014, <http://sputniknews.com/military/20141016/194157367/Russian-Strategic-Missile-Forces-Cybersecurity-Units.html>
- Rid, Thomas and Peter McBurney, “Cyber Weapons”, *RUSI Journal*, February/March 2012, vol. 157, no. 1 pp. 6–13, https://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf
- Robinson, Neil and Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle, Pablo Rodriguez, “Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)”, Rand Europe, 2013, http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR286/RAND_RR286.pdf

- Russia. "Military Doctrine of the Russian Federation" (*Voennaya doktrina Russkoi Federatsii*), December 2014,
<http://news.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf>
- Russia. "The Military Doctrine of the Russian Federation", 5 February 2010, translation, Carnegie Endowment,
http://carnegieendowment.org/files/2010russia_military_doctrine.pdf
- Russia. Federal Government. Order on the Signing on an Agreement between the Russian Federation and the People's Republic of China on Cooperation in the Field of Securing International Information Security, (in Russian), Moscow, 30 April 2015,
<http://pravo.gov.ru/laws/acts/34/555656451088.html>
- Sharma, Amit "Cyber Wars: A Paradigm Shift from Means to End", 2009, available at
<https://ccdcoe.org/publications/books/VirtualBattlefield.pdf>
- Stone, Steven W. "Factors Influencing Agility in Allocating Decision-Making Rights for Cyberspace Operations", 20th ICCRTS Paper 096, June 2015,
<http://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/54da5be5e4b0e9d26e577151/1423596517506/096.pdf>
- United Nations. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (UN GGE 2015), A/70/174, 22 July 2015,
http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
- United Nations. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/69/723, 13 January 2015,
<https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf>
- United States. Cyber Command, "Beyond the Build: Delivering Outcomes through Cyberspace", U.S. Department of Defence, Washington DC, June 2015,
http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf
- United States. Department of Defense, "*Quadrennial Defense Review Report*", 2006,
www.archive.defense.gov/pubs/pdfs/QDR20060203.pdf
- _____. "Department of Defense Strategy for Operating in Cyberspace", Washington DC, 2011, p. 11, <http://www.defense.gov/news/d20110714cyber.pdf>
- _____. "DoD Cyber Strategy", Washington DC, 2015,
http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
- _____. *Department of Defense Law of War Manual*, Washington DC, 2015, p.995,
<http://www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf>
- United States. Director of National Intelligence, "Global Trends 2015: A Dialogue about the Future with Non-Government Experts", NIC2000-2, December 2000,
http://www.dni.gov/files/documents/Global%20Trends_2015%20Report.pdf
- _____. "Industry Snapshot: Summary of Partner Responses to the FY 2015-2019 IC S&T Investment Landscape," Washington DC, 2015,
<http://www.dni.gov/files/documents/atf/In-STeP%20-%20Industry%20Snapshot.pdf>
- _____. "Statement for the Record, Worldwide Cyber Threats, House Permanent Select Committee on Intelligence", James R. Clapper, Director of National Intelligence, 10 September 2015,
<http://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf>

- _____. Remarks as delivered by The Honorable James R. Clapper, Director of National Intelligence, Opening Statement to the Worldwide Threat Assessment Hearing, Senate Armed Services Committee, Thursday, 26 February 2015, <http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee>
- United States. House of Representatives. Science Subcommittee on Energy And Science Subcommittee On Research And Technology, Written Testimony of Mr. Brent Stacey, Associate Laboratory Director for National & Homeland Security, Idaho National Laboratory, 21 October 2015, p.3, <http://docs.house.gov/meetings/SY/SY20/20151021/104072/HHRG-114-SY20-Wstate-StaceyB-20151021.pdf>
- United States. Joint Chiefs of Staff (JCS), *Cyberspace Operations*, 2013, JP 3-12R, www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf
- _____. *Information Operations*, 2012, JP 3-13, www.dtic.mil/doctrine/new_pubs/jp3_13.pdf
- United States. Space Command, “Strategic Master Plan FY06 and Beyond”, 2003, www.wslfweb.org/docs/final%2006%20smp--signed!v1.pdf
- United States. The National Defense Strategy of the United States of America, 2005, www.wslfweb.org/docs/final%2006%20smp--signed!v1.pdf
- United States. The White House. “Presidential Policy Directive 20: U.S. Cyber Operations Policy”, 2012, available at: <http://fas.org/irp/offdocs/ppd/ppd-20.pdf>
- _____. “Readout of Senior Administration Officials’ Meeting with Secretary of the Central Political and Legal Affairs Commission of the Communist Party of China Meng Jianzhu”, 12 September 2015, <https://www.whitehouse.gov/the-press-office/2015/09/12/readout-senior-administration-officials-meeting-secretary-central>
- World Economic Forum (WEF), *Global Information Technology Report 2015*, New York: Oxford University Press, for the World Economic Forum and others. Available at: http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf