MP-IDSA Monograph Series
No. 73 November 2021

LEVERAGING CYBER POWER

A Study of the Approaches and Responses of the Major Powers

Cherian Samuel

MP-IDSA Monograph Series
No. 73 November 2021

Leveraging Cyber Power: A Study of the Approaches and Responses of the Major Powers

Cherian Samuel

MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर परिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

ISBN: 978-93-82169-99-4

Disclaimer: The views expressed in this Monograph are those of the author and do not necessarily reflect those of the Institute or the Government of India.

First Published: November 2021

Price: 200/-

Published by: Manohar Parrikar Institute for Defence Studies and Analyses
No.1, Development Enclave, Rao Tula Ram Marg, Delhi Cantt., New Delhi - 110 010
Tel. (91-11) 2671-7983
Fax.(91-11) 2615 4191
Website: http://www.idsa.in

Layout & Cover by: Geeta Kumari

Printed at: KW Publishers Pvt Ltd
4676/21, First Floor, Ansari Road
Daryaganj, New Delhi 110002, India
Phone: +91 11 43528107
www.kwpub.in

Contents

Chapter 1

Introduction

Much study has gone into the analysis of the concept of national power, and all the different components and variables that can impact both its development and its utilisation. An assessment of national power serves to locate a country's relative strengths and weaknesses *vis-à-vis* peer competitors in various fields, from military to economic to social cohesion. The traditional bases of national power have included the economy, military capabilities, the science and technology base and national resources including physical, human and knowledge resources and infrastructure. The arrival of the Information Age was widely seen as a momentous development, as revolutionary as the Industrial Age, with information processing regimes replacing manufacturing as the source of wealth and economic growth. Cyber and information technologies have added a new dimension to the various components of national power, creating both new dynamics as well as new sources of vulnerabilities. They have also become key components in the formulation and execution of national policy. They also connect across all the key bases of national power and act as a force multiplier, creating new synergies and unleashing new forces. Therefore, there have been calls to reassess a country's national power through the prism of its cyber capabilities and to include new variables such as aptitude or innovation indexes and the quality of the knowledge base.[1] As will be seen, there are ongoing attempts to quantify and reassess national power based on these variables but these efforts have had mixed results since many of them are not easy to quantify, and the relative relevance of these variables keep changing along with advances in technology and the uses to which it is put.

---

[1] Ashley J. Tellis, Janice Bially, Christopher Layne and Melissa McPherson, *Measuring National Power in the Post-Industrial Age*, Santa Monica, CA: RAND Corporation, 2000. http://www.rand.org/pubs/monograph_reports/MR1110.html

Conceptualising and measuring cyber power is a very difficult proposition. Over the years, attempts have been made to rank countries on the basis of their "cyber power", which was defined by the Economist Intelligence Unit as "the ability to withstand cyber-attacks and the ability to deploy the digital infrastructure necessary for a productive and secure economy". An early index in 2014 ranked the G20 countries on a variety of parameters, constructed from 39 indicators and sub-indicators that measured specific attributes of the cyber environment across four drivers of cyber power: legal and regulatory framework; economic and social context; technology infrastructure; and industry application. India ranked 17th in this index.[2] Another matrix, the Australian Strategic Policy Institute's annual *Cyber Maturity in the Asia–Pacific Region* report had a slightly different approach, but it still measured on the basis of indicators such as the prevalence of cybercrime, role of the military, international engagement and an assessment of cyber governance. India's overall score here was brought down by factors such as inadequate capabilities to deal with cybercrime, as also the fact that the military was yet to build up capabilities or be assigned a role in "cyberspace, policy and security".[3] A third index, the Global Cybersecurity Index brought out by the International Telecommunications Union (ITU) measures the countries' commitment to cybersecurity at a global level. This commitment is assessed across five "pillars": (i) Legal Measures, (ii) Technical Measures, (iii) Organisational Measures, (iv) Capacity Building and (v) Cooperation.[4]

---

[2] *EIU-Cyber Power Index* 2014, p. 2, available at https://docplayer.net/35677178-Cyber-power-index-findings-and-methodology-an-economist-intelligence-unit-research-program-sponsored-by-booz-allen-hamilton.html, accessed on 7 July 2021.

[3] Fergus Hanson et al., "Cyber Maturity in the Asia Pacific Region 2017", *Report*, Australian Strategic Policy Institute, 12 December 2017, available at www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017, accessed on 20 January 2018.

[4] International Telecommunications Union, *Global Cybersecurity Index*, available at www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, accessed on 3 July 2021.

Whilst the 2018 Index ranked India at 24, the 2019 Index saw a precipitous fall in India's ranking to 47; the most recent 2020 Index bringing India's ranking up to 10 indicates the difficulty in using such rankings as a consistent measurement. Yet another of these indices, the Belfer Centre's National Cyber Policy Index 2020 tried to address many shortcomings of the previous rankings and present a more comprehensive ranking based on a quantitative and qualitative analysis of various indicators of cyber power. The Index graded 30 countries by drawing up a score based on how well they score on two broad parameters, intent and capability, to undertake seven broad objectives: (1) Surveilling and Monitoring Domestic Groups; (2) Strengthening and Enhancing National Cyber Defences; (3) Controlling and Manipulating the Information Environment; (4) Foreign Intelligence Collection for National Security; (5) Commercial Gain or Enhancing Domestic Industry Growth; (6) Destroying or Disabling an Adversary's Infrastructure and Capabilities and (7) Defining International Cyber Norms and Technical Standards.

This monograph looks at how major powers have tried to pursue three objectives, viz. (1) strengthening or enhancing national cyber defences, (2) striving to shape the international cyber environment by leveraging economic and technological capabilities and (3) through defining and evangelising international cyber norms. It drills down further on these three objectives to assess how much countries have been able to actualise them in their endeavours to maintain their dominance in this new domain. Specifically, these include: (1) establishing cyber commands, (2) market and technology regulation and denial mechanisms and (3) using international fora to push specific points of view in the global conversation on establishing norms in cyberspace. A section on the cybersecurity preparedness of the countries of the South Asian region is incorporated to highlight those vulnerabilities and deficient capacities and capabilities which give the major powers an opening to pursue their objectives.

Chapter 2

Military and Cyber Power

Over the years, a number of countries have set up a variety of military structures from cyber commands to smaller agencies and formations. These variations are largely on account of several factors. The role of the military in securing cyberspace is yet to be crystallised as there are fears that this would lead to cascading effects, resulting in the militarisation of cyberspace. The debate is still on as to whether an incremental approach is preferable over a big-bang approach. The invisible nature of cyberweapons means that establishing a cyber command does not have the same deterrent effect as establishing military divisions or adding lethal weaponry or new technologies to an arsenal which could have a force multiplier effect.

Whilst the military has been a key component of national power, military establishments themselves have had a difficult time dealing with the whole domain of cyber-warfare because this new domain does not fit comfortably with existing doctrines and strategies. Much of what we have come to associate with warfare, including weapons, terrain, laws of war, deciding targets, quantifying damage, etc., are less relevant in a cyber environment. Adapting the military to the cyber domain raises a lot of tough questions. How do you distinguish between a civilian and a military target? Is the duty of the military only to defend its networks or should it go beyond that? Do these duties apply only in wartime or also in peacetime? How does one deal with the overlap with civilian agencies? How does one undertake offensive missions in a domain without borders but where the collateral damage can affect other critical infrastructure in other countries? Militaries have been slow to address these issues even internally at an apex level for various reasons: the domain does not fit into the traditional conceptualisations of military activity, no role for the military has been articulated by the political leadership, and the intelligence community has filled up the vacuum. The problem for most militaries is that they are confronted with a new area of operations that is unlike any of the existing domains of land,

sea, air or even the newer domains like space. The nearest equivalent is communications and Information Warfare (IW), which has always been an adjunct of traditional warfare.

One can discern some of that struggle in the changing US definitions of cyberspace over the years. If in 2003, the reigning definition was that "Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fibre optic cables that allow our critical infrastructures to work",[5] by 2013, that definition—which conceived of cyberspace as merely an enabling network—had changed, bringing it front and centre. The 2013 definition described it as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[6]

Cyberspace has also become a domain that services other domains operated by the military. As a consequence, adversaries can impact these other domains through actions and operations in cyberspace. Effects can be calibrated from disruption to destruction, but so far even the most extreme form of destruction has been relatively minor and below the threshold of use of force and armed attack.

As in other areas, cyberspace has also impacted the traditional military domain of IW, a concept that even finds mention in ancient texts such as the *Arthasashtra*.[7] If much of what was carried out earlier was psychological warfare, the invention of new communications technologies since the 18th century have led to newer forms such as electronic warfare and cyber-warfare coming within its rubric. Thus,

---

5 US, White House, *The National Strategy to Secure Cyberspace,* Washington D.C., 2003.

6 Pentagon, *DOD Dictionary of Military and Associated Terms*, March 2013.

7 Malay Mishra, "Kautilya's *Arthashastra*: Restoring its Rightful Place in the Field of International Relations", *Journal of Defence Studies*, Vol. 10, No. 2, April–June 2016, pp. 77–109.

for the military, IW has become an amalgamation of cyber, electronic and psychological warfare.

In the face of difficulties in devising new doctrines and strategies to deal with this evolving space, militaries have fallen back on adapting old doctrines, terminologies and strategies to the new space. This can again best be seen in the strategies of the US military which has had a long legacy of incorporating IW into its military strategy. The military's goal has been to achieve dominance in the information domain/ environment through offensive and defensive information operations. This was an attainable task for electronic warfare where the electromagnetic spectrum was a limited environment, and the only considerations were the laws of physics. The spectrum had become an important enabler of modern warfare, facilitating communications and the collection and dissemination of information. Whilst information operations are, therefore, a regular peacetime activity, militaries also have to be prepared for electronic warfare, both as a peacetime and wartime activity. The goal of electronic warfare is to effectively maintain operational continuity of one's own electromagnetic spectrum whilst disrupting the adversary's ability to use the spectrum. "EW resources are used to monitor the adversary's activities in the EMS, indicate adversary's strength and dispositions, give warning of adversary's intentions, deceive and disrupt sensors and C2 processes, and safeguard the friendly use of the EMS."[8] The US military distinguishes between the nomenclature thus:

> Cyberspace operations are composed of the military, intelligence, and ordinary business operations of the DOD in and through cyberspace. Military cyberspace operations use cyberspace capabilities to create effects that support operations across the physical domains and cyberspace. Cyberspace operations differ from information operations (IO), which

---

[8] S.R.R. Aiyengar, "Exploiting the Electro-magnetic Spectrum in Jointmanship", *Journal of Defence Studies*, Vol. 1, No. 1, August 2007.

> are specifically concerned with the use of information-related capabilities during military operations to affect the decision making of adversaries while protecting our own. IO may use cyberspace as a medium, but it may also employ capabilities from the physical domains.[9]

The term "operations" is often used in the military context, where it means to carry out a particular objective, which is a targeted, well-planned exercise to achieve a particular task. The term "cyber operations" is more of a strategic terminology *prima facie*, as the usage of this term is not common compared to other cyber hyphenated words like cyber-attacks, cyber-espionage and cyber-warfare. The interpretation of cyber operations is quite open as nation-states have just started adopting the terminology to their doctrines and strategies in cyberspace. The term takes on additional connotations in the cyber domain where cyber operations need not necessarily be confined to a wartime situation. The legality of such operations is defined in statutory and customary international law with different sets of laws applicable for both war and peacetime.

Conceptualisation by the Military[10]

The US military has been at the forefront of doctrinal conceptualisation in all domains and cyberspace is no exception. The earliest version of the US Department of Defense (DoD) directive on IW in 1992 defined it as:

> the competition of opposing information systems to include the exploitation, corruption, or destruction of an adversary's information systems through such means as signals intelligence

---

[9] Congressional Research Service, *Defense Primer: Cyberspace Operations*, 18 December 2018, available at https://crsreports.congress.gov/product/pdf/IF/IF10537/3, accessed on 21 January 2019.

[10] The following section incorporates research carried out in the course of undertaking a project for the Ministry of Electronics and Information Technology.

> and command and control countermeasures while protecting the integrity of one's own information systems from such attacks.[11]

Command and Control Warfare (C2W) was created as a subset encompassing the integrated use of Psychology Operations (PSYOP), military deception, operations security (OPSEC), Electronic Warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary Command and Control (C2) capabilities while protecting friendly C2 capabilities against such actions. Command and Control Warfare in addition to being an application of IW in military operations is also a subset of IW. Command and Control Warfare applies across the range of military operations and at all levels of conflict, making it both offensive and defensive.

Publicly, the term was rephrased as Information Operations (IO) both to deflect criticism that the domain was being militarised and in recognition of the fact that these activities would also take place in peacetime. Information operations were further sub-divided into Computer Network Attack (CNA) and Computer Network Defence (CND), collectively called Computer Network Operations (CNO). Concurrently, there was the understanding that these went beyond being an enabler of traditional military operations to be a "core capability" of next-generation military forces.

The next phase recognised that such operations went beyond information and computers, encompassing the entire network and the end-point devices that depend on the integrity and availability of the network. Computer network operations stem from the increasing use of networked computers and supporting IT infrastructure systems by military and civilian organisations. Computer network operations, along

---

[11] Michael Warner, "Notes on Military Doctrine for Cyberspace Operations in the United States", *The Cyber Defense Review*, 27 August 2015, available at cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/, accessed on 28 April 2016.

with EW, is used to attack, deceive, degrade, disrupt, deny, exploit and defend electronic information and infrastructure. Transitioning from strategic to tactical targets and operations has also been difficult. Whilst strategic missions have long timeframes and are undertaken after in-depth planning and scenario building, tactical missions are time-sensitive and offer very little opportunity to space out the cyber kill chain.[12] Computer Network Exploitation (CNE), defined as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks" was added to the mix, along with the understanding that such activities could be undertaken even by all manner of adversaries, ranging from individuals to nation-states. Information operations and CNO were subsequently encapsulated within cyberspace operations.

The classified US Presidential Policy Directive 20 (PPD 20) issued in October 2012, which was leaked by the *Guardian* newspaper in June 2013, while discussing cyber operations and command and control, made no mention of cyber weapons. It however noted that:

> The United States Government shall integrate DCEO (Defensive Cyber Effect Operations) and OCEO (Offensive Cyber Effect Operations) as appropriate, with other diplomatic, informational, military, economic, financial, intelligence, counterintelligence, and law enforcement options, taking into account costs, risks, potential consequences, foreign policy and other policy considerations.[13]

As per PPD 20, defensive cyber operations are activities to defend or protect against "imminent threat or ongoing attack or malicious cyber activity" against the networks of the US government. A defensive cyber

---

[12] Michael Klipstein and Michael Senft, "Cyber Support to Corps and Below: Digital Panacea or Pandora's Box?", *Small Wars Journal*, available at www.smallwarsjournal.com/jrnl/art/cyber-support-to-corps-and-below-digital-panacea-or-pandora%E2%80%99s-box, accessed on 10 October 2017.

[13] US White House, Presidential Policy Directive 20, *US Cyber Operations Policy,* October 2012, available at http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text, accessed on 8 August 2017.

operation does not intend to damage or degrade the infrastructure, assets, communication channels or critical information infrastructure of other states. These operations are carried out in defence of United States' own networks, infrastructure and cyber assets from any untoward incident or a breach.

Offensive Cyber Operations

Offensive operations in cyberspace require unilateral efforts by the states to inflict damage to other states' infrastructure or to degrade it severely if the need to do so arises. These capabilities display the "power" of the state to conduct such operations. The US PPD 20 defines these operations as capabilities to advance US 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". The capabilities required are much more complex than those required for defensive cyber operations. The US also perceives offensive cyber operations as a deterrent to a host of threats to its national interest in the cyber realm.

Building capacity and capability to conduct operations in cyberspace is a resource-intensive exercise as it requires specialised skill-set. The capabilities required to conduct a cyber operation need sustained planning, effort and financial resources in addition to the desired skill-set. In order to realise such capabilities, states have established cyber commands under the armed forces. Usually, the armed forces defend a nation state in the case of an external aggression or war. On similar lines, given the grave implications of cyber threats to the national security, armed forces are increasingly playing an important role in devising operational responses to the acts of war or aggression in cyberspace.

Along with such capacities, the "intent" of the state is warranted to exercise these capabilities in response to an act of aggression, which subsequently has many implications for international peace and stability.

Other Conceptualisations of Offensive Cyber Operations

The intrinsic difficulties in modifying existing doctrines for cyberspace to have a uniform and harmonised way of operating in different

domains is exemplified by the conceptual gymnastics of the US military. By way of comparison, China emphasises on sovereignty in cyberspace and perceives it as an extension of its national territory. The National Cybersecurity Strategy document released in 2016 emphasised this aspect, noting that "[China] will regulate internet activities within the country's sovereignty, protect the safety of information facilities and resources and take all means, including economic, administrative, technological, legal, diplomatic and military, to safeguard China's cyberspace sovereignty".[14] The major cybersecurity challenges identified included attacks meant to discredit political system, incite social disorder or paralyse the financial or telecom infrastructure. The military had a key role to play in China's cybersecurity with a Chinese analyst noting, "Just like [force] will be deployed on the front line for attacks on China's territory, military forces will be used for the same defence purposes in cases such as key informational infrastructure being attacked."

However, the operational capabilities of the Chinese military in this regard are not available in the public domain other than conceptual papers, think tank articles and assessments by US intelligence agencies.

The Chinese military has conceptualised cyberspace as an arena of continuous warfare. This was first enunciated in a 1999 treatise titled "Unrestricted Warfare" by two Colonels of the Chinese army.

The authors began by observing:

> Does a single "hacker" attack count as a hostile act or not? Can using financial instruments to destroy a country's economy be seen as a battle?... Obviously, proceeding with the traditional definition of war in mind, there is no longer any way to answer the above questions. When we suddenly realize that all these non-war actions may be the new factors constituting future warfare, we have to come up with a new name for this new form

---

[14] Zhuang Pinghui, "China Sees PLA Playing Key Role in Cyberspace", *South China Morning Post*, 20 July 2018, available at www.scmp.com/news/china/policies-politics/article/2057500/china-sees-pla-playing-frontline-role-cyberspace, accessed on 25 December 2018.

> of war: Warfare which transcends all boundaries and limits, in short: unrestricted warfare.
>
> If this name becomes established, this kind of war means that all means will be in readiness, that information will be omnipresent, and the battlefield will be everywhere. [I]t also means that many of the current principles of combat will be modified, and even that the rules of war may need to be rewritten.[15]

This conceptual integration of peacetime and wartime has been followed by other concepts such as "military civil fusion" and "pre-emptive cyber-attack". The seamlessness underlined in Chinese conceptions of cyber operations contrasts with US formulations that distinguish between defensive and offensive operations and the various operational and legal considerations that have to be taken into account while distinguishing between these operations.

The Chinese Military Strategy 2015 characterised the military's role thus:

> Cyberspace has become a new pillar of economic and social development, and a new domain of national security. As international strategic competition in cyberspace has been turning increasingly fiercer, quite a few countries are developing their cyber military forces. Being one of the major victims of hacker attacks, China is confronted with grave security threats to its cyber infrastructure. As cyberspace weighs more in military security, China will expedite the development of a cyberforce, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability.[16]

---

15 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America*, Panama: Pan American Pub., 2002, p. 5.

16 *China's Military Strategy*, White Paper, The State Council, The People's Republic of China, 27 May 2015, available at english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm, accessed on 20 July 2021.

The reorganisation that took place in 2015 sought to integrate cyber capabilities spread across the military as well as to unite cyber, aerospace and electronic warfare capabilities under one centralised command. The Informatization Department that was created in 2011 facilitated the integration and once the task was completed, it was downsized, and its units integrated into other departments such as the Information and Communications Bureau and the Strategic Support Force.[17]

Other countries have also taken steps to conceptualise and transform their militaries by integrating cyber capabilities and raising new units within their militaries. In 2010, Australia established a Cyber Security Operations Centre (CSOC) within the Australian Signals Directorate to tackle threats emanating from Information and Communication Technologies (ICT) following a recommendation in the 2009 White Paper on Defence.[18] In 2014, this centre evolved into the Australian Cyber Security Centre (ACSC) to give it a broader focus beyond the military. It combined together the expertise of the Defence Intelligence Organisation, Australian Security Intelligence Organisation (ASDIO), CERT Australia, the Australian Federal Police and the Australian Crime Commission (ACC).[19] The Centre, after being merged with CERT Australia, was subsequently brought within the ambit of the Australian Signals Directorate which was a part of the Department of Defence.[20]

---

17 Elsa Kania, "China's Strategic Support Force: A Force for Innovation?", *The Diplomat*, 18 February 2017, available at thediplomat.com/2017/02/chinas-strategic-support-force-a-force-for-innovation/, accessed on 21 August 2018.

18 White Paper 2017, Department of Defence, Australian Government, available at www.defence.gov.au/whitepaper/2009/, accessed on 21 August 2018.

19 Rohan Pearce, "From Signals to Cyber: Inside the Transformation of the Australian Signals Directorate", *Computerworld*, 25 October 2018, available at www.computerworld.com.au/article/648710/from-signals-cyber-inside-transformation-australian-signals-directorate/, accessed on 21 November 2018.

20 The Australian Signals Directorate (ASD) is a part of the 5 Eyes Alliance which includes US (NSA-National Security Agency), UK (GCHQ-Government Communication Headquarters), Canada (CSEC-Communication Security Establishment Canada) and New Zealand (GCSB-Government Communication Security Bureau).

The Defence White Paper of 2016 also called for the establishment of an information warfare unit.[21] It was to be a joint command, reaching a strength of 900 in 10 years. [22] Australia has also been regular in publishing cybersecurity strategies with the first one published in 2016, followed by a second iteration in August 2020. The strategy outlines means and mechanisms of strengthening the security and resilience of the country's critical infrastructure, and of securing families and businesses online. It also lays out the budgeting for the programmes. What is of relevance here is that much of the implementation is to be done by the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC).

The UK government's position has been that the principles of deterrence are as applicable in cyberspace as they are in the physical sphere, and therefore the full spectrum of UK's capabilities will be used to deter adversaries. Whilst much of the focus has been on enhancing the capabilities of the century-old signals intelligence organisation, Government Communications Headquarters (GCHQ), and its cybersecurity offshoot, the National Cyber Security Centre (NCSC), the military's efforts have centred around bringing in cyber as part of a broader effort to restructure the military in line with changing threats and technological developments. To this end, the Force Troops Command (FTC) was set up in 2013 by amalgamating the army's specialist brigades, including the 1st Intelligence, Surveillance and Reconnaissance Brigade, 1st (United Kingdom) Signal Brigade, 11th Signal Brigade & HQ West Midlands and 77th Brigade.[23] The thrust of the FTC was to coordinate "Information Manoeuvre", fusing and

---

[21] White Paper 2016, Department of Defence, Australian Government, available at http://www.defence.gov.au/whitepaper/docs/2016-defence-white-paper.pdf, accessed on 21 August 2018.

[22] Ashlynne McGhee, "900 Soldiers for New Cyber Battle Force", *ABC News*, 30 June 2017, available at www.abc.net.au/news/2017-06-30/cyber-warfare-unit-to-be-launched-by-australian-defence-forces/8665230, accessed on 20 July 2018.

[23] *Force Troops Command (FTC) Handbook,* Ministry of Defence, United Kingdom, Upavon: Headquarters Force Troops Command, 2017, p. 4.

synchronising multiple information-centric capabilities available in both civilian and military agencies in order to provide "improved understanding; enhanced methods of communication; more nuanced and innovative means to influence target audiences; and more sophisticated ways to protect our people, equipment, infrastructure and data."[24] The objective of this concept was to synergise five information capabilities: "Intelligence, Surveillance and Reconnaissance (ISR or Intelligence); Communications and Information Systems (CIS or Networks); Cyber Electromagnetic Activity (CEMA or Cyber); Information Activity and Outreach (IA&O or Influence); and Counter Intelligence & Security (CI or Security)."[25] As the handbook further noted, these capabilities are not typical "chains of command", they are distributed between different government departments and the Services.[26] Achieving this synergy has proved to be the bane for most militaries; in 2019, the Force Troops Command was renamed as the 6th Division as per the Army 2020 restructuring. A dedicated cyber security regiment was formally raised in June 2020, consisting of over 250 personnel drawn largely from the army, but also including specialist personnel from the navy and the air force. This was a part of the ARMY 2020 reorganisation and force modernisation, elaborated in a speech by the Chief of the Defence Staff in December 2019 where he explained the re-organisation in the following words:

> Our modernised force will be framed through the integration of five domains—space, cyber and information, maritime, air and land…. It will develop and generate the capabilities we need to operate successfully in this sub-threshold context—or grey zone, as some call it—including space, cyber, special operations and information operations.

France has conceived of cyber defence as having a civilian and military component through several White Papers and strategic reviews. The

---

[24] Ibid.

[25] Ibid., p. 9.

[26] Ibid.

emphasis in the early years was on the civilian component with no role for the military. The 2013 White Paper on Defence did cover cyber threats from various threat actors though there was no mention of a role for the military. That notwithstanding, there was some out-of-the-box thinking going on within the military and the government with one of the innovations being the idea that military and civilian cyber specialists should be located in the same building for better coordination in the event of networks going down. It was only in 2016 that a Cyber Command was formed with the French National Strategy of 2018, spending considerable effort in laying out the various roles and responsibilities and operational chains and ensuring that there was no overlap of responsibilities. The French Military Cyber Strategy brought out in 2019 laid out the military's perception of its role in cyberspace. Among the notable elements was the uniformity in thinking about cyberspace as an arena of permanent confrontation that ran counter to the Western military's sharp delineation between peacetime and wartime, as seen even in the Laws of Armed Conflict.

Discussions within the Indian establishment on the need for cyber capabilities have been going on for more than a decade with then prime minister Manmohan Singh talking of threats from the cyber domain in his addresses to the Combined Commanders Conference in 2011 and 2012. The Naresh Chandra Committee of 2011 had recommended setting up a cyber command to the establishment in 2011 and in 2014, and the then Chief of Army Staff Gen. Bikram Singh said that the military had forwarded a note on the establishment of a Cyber Command to the Cabinet Committee on Security. In the event it was a more truncated Defence Cyber Agency (DCA) to be headed by a two-star officer which was announced in 2018. Whilst no details have been forthcoming on the terms of reference of the DCA, it is presumed to have defensive as well as offensive capabilities.

On the conceptual level, the two military documents that have been released in recent times and refer to cyberspace are the Joint Doctrine released in 2017 and the Land Warfare doctrine released in 2018. The Joint Doctrine is quite vague on cyber operations, simply noting that "A comprehensive Cyber force structure drives capabilities in cyber war fighting and wins Network Centric Wars (NCW)"and that "Exploiting information technology and Integrated Reconnaissance,

Surveillance and Command, Control, Communications, Computers, Information and Intelligence systems will win battles."[27] Other than acknowledging that "in the globalised world economy of today, cyberspace has probably become the single-most important factor that provides necessary linkages, stores information, facilitates business transactions and acts as an effective medium for instant delivery of services" and that "high value cyber assets make the Critical Information Infrastructures of the Nation, which must be protected at all costs, to enable the core and routine state businesses function uninterrupted" there is no elaboration on its role in cyberspace.[28] The impression one gets from the document is that the military does not perceive a role for itself other than in protecting its own networks and the Ministry of Defence through the Defence Information Assurance and Research Agency which is "the nodal agency mandated in dealing with all cyber security needs of the Tri-Services and MoD".[29] This impression is reinforced by the fact that the document call for the creation of a Defence Cyber Agency as against the previous calls for a Cyber Command.

The Land Warfare doctrine published a year later is more upfront about the need for offensive capacities in the cyber/information domain, noting that "The Indian Army will enhance capabilities to address the challenges of non-contact domains of conflict viz. cyber, space and information as a component of our National Strategy for noncontact warfare to cause unaffordable losses to potential adversaries" and "due to increased threat of hybrid warfare, the Indian Army will [have to] prosecute operations with designated forces, equipped and mandated to effect attacks/ retaliation in the Information Warfare (IW) domain".[30] Cyberwarfare is brought within the ambit of

---

[27] *Joint Doctrine Indian Armed Forces*, Headquarters, Indian Defence Staff, April 2017, p. 70.

[28] Ibid., p. 40.

[29] Ibid., p. 70.

[30] *Land Warfare Doctrine 2018,* Indian Army, p. 15.

information warfare with the other two components being Electronic Warfare (EW) and Psychological Warfare (PSYW).[31]

However, it is not clear whether there will be integration of units from each of these subdivisions as has been carried out by other militaries. Whilst the need to develop capabilities in the cyber domain has been taken cognisance of, much of the military's thinking remains to be fleshed out. It is also clear as seen in the next chapter that, being a new domain, considerable experimentation has to be done to arrive at an optimum framework for the military. Statements emanating from the top leadership in the recent past show that there is adequate cognisance of the threat.[32] The ongoing efforts at theaterisation provide a good opportunity to fashion a viable cyber component for the Armed Forces, whether it be a joint Command or a Unified Command. The experiences of other militaries show that each military will have to fashion a cyber component unique to its requirements and existing capacities and capabilities.

---

[31] Ibid., p. 10.

[32] Abhishek Bhalla, "China Capable of Disrupting Systems by Launching Cyber Attacks on India: Cds Bipin Rawat", *India Today,* 7 April 2021, available at https://www.indiatoday.in/india/story/china-cyber-attacks-india-cdsgeneral-bipinrawat-1788382-2021-04-07, accessed on 15 July 2021.

Chapter 3

A Comparative Study of the Evolution of US Cyber Command, French Comcyber and China's Strategic Support Command

This chapter examines the evolution of Cyber Commands in three countries with differing doctrines within their respective militaries. The attempts to incorporate cyber into the existing command and control structures either by restructuring the existing set-up or by a complete root and branch overhaul have met with mixed success.

US Cyber Command

US Cyber Command was established in 2009 following an unprecedented cyber-attack on military computers that was attributed to Russia.[33] It is staffed through the Cyber Mission Force, which was set up in 2012. The cyber environment has proved to be hugely complicated and multi-dimensional, and therefore, while the objectives in both electronic and cyber-warfare, which are, "Deny, deceive, disrupt, destroy, or exploit the adversary's capability to communicate, monitor, reconnoitre, classify, target, and attack"[34] might be similar, it is not as

---

[33] William J. Lynn, "Defending a New Domain", *Foreign Affairs*, 30 May 2014, available at www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain, accessed on 21 May 2017; Brian Knowlton, "Military Computer Attack Confirmed", *The New York Times*, 25 August 2010, available at www.nytimes.com/2010/08/26/technology/26cyber.html, accessed on 16 April 2018.

[34] Joint Doctrine for Electronic Warfare, U.S. Department of Defense, 2017, p. F2, available at fas.org/irp/doddir/dod/jp3_51.pdf, accessed on 13 March 2018.

easy to follow through on these objectives in cyberspace. As with the former, the tactics and procedures in cyber-warfare have been given terms like computer network attack, computer network exploitation and computer network defence. Even though the United States declared cyberspace as the Fifth Domain of Warfare in 2010, it has been difficult for militaries grounded in the more physical domains of land, sea, air and space, to consider it as nothing more than a domain that supports other domains, and not a major theatre of conflict in itself. The evolution of this domain has also led to different organisations taking core responsibility for managing and utilising the domain, with policy makers unable to take a decision on giving the dominant role to any one organisation. This applies to the military domain as well, with different organisations and agencies responsible for undertaking defence and offense roles respectively. Intelligence organisations, either from the civilian or the military stables have become *de facto* leading agencies by virtue of the fact that much of state-sponsored activity has revolved around cyber exploitation, which is, espionage and related activities. The transition to other agencies has proved to be difficult, as seen in the case of the United States, where the National Security Agency was conjoined with the Cyber Command when it was set up and subsequent efforts to delink the two have not succeeded.

This brings up the issue of responsibilities; US CyberCom defines its core responsibilities as "Defending DoD networks, providing support to combatant commanders for execution of their missions around the world, and strengthening our nation's ability to withstand and respond to cyber-attack."[35] Of these, whilst the first two are relatively straightforward, the third is ambiguously worded, possibly because any more direct wording would bring the issue of overlap with other agencies, such as the Department of Homeland Security and the Department of Justice, as well as the legality of DoD's domestic operations. This dichotomy was again seen reflected in the DoD's Cyber

---

[35] US Cyber Command, Mission and Vision, available at https://www.cybercom.mil/About/Mission-and-Vision/, accessed on 17 May 2017.

Strategy and the Command Vision for Cyberspace[36] published in 2018 wherein it stated, *inter alia,*

> that the Department seeks to pre-empt, defeat, or deter malicious cyber activity targeting US critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD's warfighting readiness or capability. Our primary role in this homeland defense mission is to defend forward by leveraging our focus outward to stop threats before they reach their targets. The Department also provides public and private sector partners with indications and warning (I&W) of malicious cyber activity, in coordination with other Federal departments and agencies.[37]

This was a continuation of the DoD's traditional mandate to only focus on external threats and leave domestic agencies to focus on internal threats. In the case of cyber, the same argument had been put forward in testimony in 2017 where the then Assistant Secretary of Defense for Homeland Defense and Global Security, Kenneth Rapuano had stated that "[T]he United States has a long normative and legal tradition limiting the role of the military in domestic affairs. This strict separation of the civilian and the military is one of the hallmarks of our democracy and was established to protect its institutions. Designating DoD as the lead for the domestic cyber mission risks upsetting this traditional civil–military balance."[38] With considerable pushback from Congress, which called for the DoD to do more, a process was set in motion to update

---

[36] See Appendix 2.

[37] "US, Department of Defense Cyber Strategy", Department of Defense, 2018, available at media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, accessed on 19 December 2018.

[38] Mark Pomerleau, "DoD Says It Shouldn't Protect Homeland from Cyberthreats; McCain Disagrees", *Fifth Domain*, 13 September 2018, available at www.fifthdomain.com/congress/capitol-hill/2017/10/19/dod-says-it-shouldnt-protect-homeland-from-cyberthreats-mccain-disagrees/, accessed on 14 September 2018.

the relevant legislation and authorities to make the military a more relevant player in cybersecurity. The Department of Defence Cyber Strategy and the White House Cyber Strategy, both published in 2018, became the new foundational documents outlining the functions and operational authorities of Cyber Command. The latter gave leeway to Cyber Command to forego restraint on offensive cyber activities with operational commanders being given permission to undertake both pre-emptive action as well as responses to developing cyber events. This marked a big change from the earlier permissions under the restricted publication PPD-20 where such actions required approval from much higher up the chain of command, as well as across agencies.[39] Whilst the earlier policy was designed to ensure that cyberspace operations of the military did not impact activities of other agencies such as the espionage agencies or affect state-to-state relations, this had apparently resulted in a gridlock for the military with the State Department using its veto powers to strike down operations even against entities like the ISIS.[40]

Cyber Commands' efforts to reinvent itself under the new mandate can be traced through successive speeches by the current head, General Nakasone, which are filled with buzzwords like *defending forward* and *persistent engagement*.[41] The academic underpinnings of these new approaches can be traced to the writings of Dr Richard J. Harknett. According to him, describing cyberspace as the fifth domain was an error in that it led to expectations that doctrines that had proven

---

[39] Adam K. Raymond, "Trump Makes It Easier for the Military to Launch Cyberattacks", *Intelligencer*, 16 August 2018, available at nymag.com/intelligencer/2018/08/trump-makes-it-easier-for-the-u-s-to-launch-cyber-attacks.html, accessed on 18 November 2018.

[40] Eric Geller and Jason Schwartz, "Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand", *POLITICO*, 16 August 2018, available at www.politico.com/story/2018/08/16/trump-cybersecurity-cyberattack-hacking-military-742095, accessed on 18 November 2018.

[41] Paul Nakasone and Olivia Gazis, *RSA Conference*, 6 March 2019, available at www.rsaconference.com/videos/strategic-competition-the-rise-of-persistent-presence-and-innovation, accessed on 15 April 2019.

successful in the other domains could be easily adapted to this domain. Unlike the others, cyberspace was an "interconnected domain in which the military must operate." Attack artefacts like source and intent and concepts like signalling and escalation dynamics which worked well in traditional domain to pinpoint attack and responses did not lend themselves well to the cyber domain.[42] Relevant provisions of the John McCain National Defense Authorization Act for fiscal 2019 gave the legislative authority to rewire Cyber Command.

The military has also struggled to incorporate cyber into its doctrine of deterrence, which has been the lodestar for ensuring the security of the homeland. Both conventional and nuclear deterrence, centred around overwhelming power have ensured peace and security for the United States since the end of the Second World War. The concept of deterrence has proved to be difficult to adapt to cyber security.

At the end of the day, it remains a fact that the US Cyber Command is still hamstrung in performing its most basic duty, that of defending and securing DoD networks.[43]

Structure of Cyber Command

The Cyber Command was fleshed out through the Cyber Mission Forces, set up in 2012. The Cyber Mission Force was further sub-divided into: (1) Cyber National Mission Force whose objectives were to monitor adversary activity and block attacks; (2) the Cyber Combat Mission Force whose mandate was to conduct military cyber operations in support of combatant commands; and (3) the Cyber Protection Force tasked with defending the "DODIN"—the DOD information

---

[42] Brad D. Williams, "Meet the Scholar Challenging the Cyber Deterrence Paradigm", *Fifth Domain,* 23 July 2017, available at www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/.

[43] Matthew Gault, "The American Military Sucks at Cybersecurity", *Motherboard*, VICE, 15 January 2019, available at motherboard.vice.com/en_us/article/7xy5ky/the-american-military-sucks-at-cybersecurity.

networks—and preparing cyber forces for combat. Cyber Support Teams were also to be in place to provide analytic and planning support to National Mission and Combat Mission teams. At its full strength, to be reached by 2016, the Cyber Mission Force was to number 133 teams, comprising 6,200 personnel with about 2,300 being hired in 2013 itself.[44] Of these, approximately 3,000 would serve on the Cyber Protection Force, about 1,000 would be staffed within the National Mission Force, and about 2,000 with the Combat Mission Force. As far as the personnel assigned to each team were concerned, the breakup was to be 60-person National Mission Teams, 40-person Cyber Protection Teams and 60-person Combat Mission Teams.[45] The 13 national mission teams were to be supported by eight national support teams, and the 27 combat mission teams with 17 combat support teams. There were to be 18 national cyber protection teams, 24 service cyber protection teams and 26 combatant command and DoD Information Network Cyber Protection Teams (CPTs).[46]

The target date for full operational capability was extended to 2018 and reaching that milestone was announced on 17 May 2018.[47] The proportion of the army and the navy in Cyber Command was at 60 per cent with air force and marines comprising the remaining 40 per

---

44 Wyatt Olson, "Cyber Command Trying to Get Running Start, Add Staff", *Stars and Stripes*, 11 December 2014, available at www.stripes.com/news/cyber-command-trying-to-get-running-start-add-staff-1.318612, accessed on 16 August 2018.

45 Aliya Sternstein, "Need a Job? Cyber Command Is Halfway Full", *Nextgov*, 6 February 2015, available at www.nextgov.com/cybersecurity/2015/02/need-job-cyber-command-halfway-full/104817/, accessed on 18 September 2018.

46 Mark Pomerleau, "Here's How DoD Organizes Its Cyber Warriors", *Fifth Domain*, 25 July 2017, available at www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/, accessed on 30 September 2018.

47 Mark Pomerleau, "Cyber Command Reaches Critical Staffing Milestone", *Fifth Domain*, 18 May 2018, available at www.fifthdomain.com/dod/cybercom/2018/05/17/cyber-commands-cyber-warriors-hit-key-milestone, accessed on 19 November 2018.

cent.[48] Inductees attended training courses that ranged between 10 and 27 months. The total budget for setting up the US Cyber Command was $2 billion.[49]

Retaining human resources has proved to be one of the biggest problems for Cyber Command, so much so that applicants were given a service incentive to retain and combat the notion that it would lead to career stagnation.[50] The army for instance, offered a service retention bonus of $7,900 to $50,400 depending on expertise and experience.[51] Though provisions were included for hiring civilian cyber talent, that was made difficult by "internal federal employment constraints regarding compensation and a comparatively slow hiring process".[52] The composition of civilians in Cyber Mission Forces was in the range of 20 per cent in 2016.[53]

---

48 Joseph Marks, "US Army, Navy Cyber Commands Ready Far Ahead of Schedule", *Defense One*, 3 November 2017, available at www.defenseone.com/threats/2017/11/us-army-navy-cyber-commands-ready-far-ahead-schedule/142287/, accessed on 18 March 2018.

49 Aliya Sternstein, "US Military Cybersecurity by the Numbers", *Nextgov*, 22 December 2016, available at www.nextgov.com/cybersecurity/2015/03/us-military-cybersecurity-numbers/107637/, accessed on 22 January 2017.

50 "Army Braces for A Culture Clash", *SIGNAL Magazine*, 4 January 2016, available at www.afcea.org/content/Article-army-braces-culture-clash, accessed on 15 November 2018.

51 David Ruderman, "Army Offers Selective Retention Bonuses to Retain Enlisted Cyber Warriors", *www.army.mil*, 29 May 2015, available at www.army.mil/article/149561/army_offers_selective_retention_bonuses_to_retain_enlisted_cyber_warriors, accessed on 18 March 2016.

52 "Cyber Chief: Army Cyber Force Growing 'Exponentially'", *www.army.mil*, 5 March 2015, available at www.army.mil/article/143948/cyber_chief_army_cyber_force_growing_exponentially, accessed on 18 May 2018.

53 "Event Coverage of 2015 AUSA Annual Meeting & Exposition", *The CyberWire*, 12 October 2015, available at thecyberwire.com/events/ausa-annual-meeting-and-exposition-2015.html, accessed on 17 June 2018.

Cyber Re-organisation in the US Army

The process of setting up Cyber Command has meant that at the same time as a new hierarchy is being created, the existing systems must be realigned and merged properly into the new setup. The reorganisation of the army to reflect the changing requirements saw the Brigade Combat Team (BCT) becoming the fulcrum. Cyber Electromagnetic Activities (CEMA) teams were created to provide support to the BCTs under a programme called CEMA Support to Corps and Below (CSCB), which was launched in 2015. Cyber Electromagnetic Activities is designed to provide tactical commanders with integrated cyberspace operations, Department of Defence Information Network Operations, electronic attack, electronic protection, electronic warfare support, spectrum management operations, intelligence, and information operations support/effects. The CSCB programme is designed to help the army define and develop cyberspace doctrine and organisation, enabling support and integration into tactical units, in synchronisation with related warfighting disciplines such as electronic warfare, information operations, network operations and intelligence. Through this programme, CEMA teams have been integrated with the BCTs at combat training centres. Integration had to be both upstream and downstream, with CEMA teams learning to work closely with the BCT, and the CEMA teams, comprising specialists from cyber, military intelligence and electronic warfare, and signals intelligence also learning to cooperate closely.[54] Whilst electronic warfare teams have already been merged with the cyber teams, efforts are also on to do the same with the information operations teams as well as to create social network analysis teams and incorporate them into the Cyber Branch.

One of the objectives of the CSCB programme has been to "game" out the types of cyber, electronic warfare and information capabilities

---

[54] "US Army Cyber-Electromagnetic Activities Teams", *Warfare Today*, 15 January 2018, available at www.warfare.today/2018/01/15/us-army-cyber-electromagnetic-activities-teams/, accessed on 18 October 2018.

required at different command levels.[55] Going forward, the exercise would be replicated at the division and corps levels through regional and joint cyber centres, and to create Expeditionary Cyber-Electromagnetic Teams (ECTs). These ECTs would form the core of the 915th Cyber Warfare Support Battalion (CWSB), which has already been raised. The CWSB would have 12 expeditionary cyber teams, each consisting of detachments with 45 personnel. These elements would be "capable of conducting localized cyber effects through the electromagnetic spectrum, rather than the IP-based operations conducted by Cyber Command, though it might have a tie-in with these forces and capabilities."[56]

French CYBERCOM

As per the strategic review of cyber defence published by the Secretary General for Defence and National Security in 2018, the cyber defence of France is organised on the principle that offense and defence have to be on separate tracks, unlike the prevailing Anglo-Saxon model that gives responsibility of cyber defence to the intelligence agencies.[57] It listed an active stance of cyber deterrence as one of the seven major principles "at the heart of France's ambition on cyber deterrence". Thus, France has conceived of cyber defence as having a civilian as well as military component.

This marked an evolution in France's policy on cybersecurity that began with the publication of a White Paper in 2009, which led to the creation

---

55 Mark Pomerleau, "What Can Cyber Do for You, the Commander?" *Fifth Domain*, 15 December 2017, available at www.fifthdomain.com/electronic-warfare/2017/12/15/what-can-cyber-do-for-you-the-commander/, accessed on 13 February 2018.

56 Mark Pomerleau, "The Army Looks to Build Up Its Cyber Arsenal", *Fifth Domain*, 7 May 2019, available at www.fifthdomain.com/dod/army/2019/05/06/the-army-looks-to-build-up-its-cyber-arsenal/, accessed on 16 October 2019.

57 *Strategic Review of Cyber Defence*, Government of France, 2018, pp. 1–14, available at www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf, accessed on 18 December 2018.

of the French National Information Systems Security Agency (ANSSI). This was followed by a National Cybersecurity Strategy in 2011, which emphasised on cyber defence with no role assigned to the military.[58] The civilian component was set up consequent to the recommendation of the 2009 Defence White Paper that a centralised body was required for cybersecurity issues. The four pillars of French cybersecurity as defined by the White Paper were: (1) to be present internationally as a cyberspace power, that is, to be present in all rule making and standard setting bodies; (2) to preserve the decision making autonomy of France through the protection of information related to its sovereignty—this has proved to be a challenge in the face of increasing cyber-espionage; (3) protect critical infrastructure; and (4) secure cyberspace for its citizens.

The ANSSI was set up as a body under the Prime Minister's Office. Though a civilian organisation, it replaced the Central Directorate for Network and Information Security (DCSSI) of the Secretariat General for National Defence (Secrétariat Général de la Défense Nationale—SGDN), reflecting its military heritage.[59] Notwithstanding that it dealt with cyber defence, it did not have any intelligence, police or judicial powers or functions. Its roles were: (1) *preventive*—defining rules for critical infrastructure, mandating audits and imposing fines for non-compliance, deploying e-IDs for government servants, running an alert network and awareness campaigns, developing school curricula for information assurance and running table-top and simulation exercises such as sending out phishing emails to top government officials to see who does not follow basic cyber hygiene etc.; (2) *advisory*—issuing best practices on securing systems, certifying products; and (3) *operational*—securing governmental communication networks, having rapid reaction teams on standby, identifying attacks on networks, limiting damage and getting them back online.

---

[58] *Information Systems Defence and Security: France's Strategy*, Government of France, 2011, pp. 1–24, available at https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf, accessed on 18 November 2017.

[59] *ANSSI*, The National Cybersecurity Agency of France, available at www.ssi.gouv.fr/en/cybersecurity-in-france/the-national-cybersecurity-agency-of-france/, accessed on 10 June 2019.

When started in 2009, it had 100 employees, which increased to 360 by 2011. This included personnel on deputation from the police and other law enforcement agencies who acted as liaisons with their parent organisations. As compared to other cybersecurity agencies and Computer Emergency Response Teams (CERTs), ANSSI has a more active approach, which has been backed up through legislative action. A proposed plan, for instance, called for ANSSI to set up detection devices on the systems of telecommunications providers to track attackers in real-time.[60]

The 2013 White Paper on Defence amplified on the cyberthreat with over 45 references through the White Paper covering cyberthreats from various threat actors. However, it did not explicitly outline a role for the military.[61] That notwithstanding, the formation of a Cyber Command was announced in December 2016 with initial funding of 2.5 billion Euros. In his speech announcing the development, the French Minister of Defence described its offensive mission as follows: "Our offensive cyber-capabilities must allow us to breach the systems and networks of our enemies to cause damage, service suspensions or temporary or definitive neutralisations."[62] In a first for a Cyber Command, a contingent of the French cyber command also marched for the country's Bastille Day celebrations in 2018.[63] The Military Planning

---

60 *Strategic Review of Cyber Defence*, Government of France, 2018, p. 7, available at www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf, accessed on 15 March 2019.

61 *White Paper on Defence and National Security* 2013, Directorate General for International Relations and Strategy, France, available at https://www.defense.gouv.fr/english/dgris/defence-policy/white-paper-2013/white-paper-2013, accessed on 17 March 2019.

62 Tom Reeve, "France Unveils Cyber Command in Response to 'New Era in Warfare'", *SC Magazine*, 16 December 2016, available at www.scmagazineuk.com/france-unveils-cyber-command-response-new-era-warfare/article/1475678, accessed on 16 March 2019.

63 Andrew Liptak, "France's Cyber Command Marched in Paris's Bastille Day Parade for the First Time", *The Verge*, 14 July 2018, available at www.theverge.com/2018/7/14/17572098/france-cyber-command-comcyber-cybersecurity-military-bastille-day-parade, accessed on 8 March 2019.

Act 2019–2025 provided for another 1,500 personnel to be added to the 2,500 recruited when the cyber command was raised.[64]

While the French National Strategy of 2018 comprehensively covers cybersecurity, it is notable for clearly delineating the responsibilities of the current and future agencies to be entrusted with cybersecurity so that there is very little overlap of their functions. Four "operational chains", protection, intelligence, judicial investigations and military action, were established to contribute to the missions of prevention, anticipation, protection, detection, attribution and reaction. The chain of command and mechanism for cooperation were also outlined in the Strategy.[65]

The French Military Cyber Strategy was brought out in January 2019 in two parts: the Ministerial Policy for Defensive Cyber Warfare and the Unclassified Elements of the Military Doctrine on Offensive Cyber Operations.[66] The latter was only partially unclassified. A reading of these documents would indicate that the purpose of publication was manifold. They laid out French redlines to serve as a deterrent against destructive cyber-attacks and made a clear distinction between defensive and offensive operations. In this sense, it can be considered as the military version of the Cyber Security Strategy with the various aspects of a cyber military doctrine being spelt out. Some aspects of the Cyber Military Strategy are seen as similar to the US Cyber Command's doctrine of persistent engagement where cyberspace is seen as an environment of permanent confrontation, including in peacetime.[67] The Public Elements document defined military offensive cyber-warfare

---

64 See https://www.defense.gouv.fr/content/download/523150/8769279/file/LPM%202019-2025%20-%20Rapport%20annex%C3%A9.pdf, accessed on 11 March 2019.

65 n. 57, p. 5.

66 See Appendix 1 for an approximate translation.

67 Stephanie Taillet, "Signaling, Victory, and Strategy in France's Military Cyber Doctrine", *War on the Rocks*, 7 May 2019, available at warontherocks.com/2019/05/signaling-victory-and-strategy-in-frances-military-cyber-doctrine/, accessed on 16 June 2019.

as "all military actions undertaken in cyberspace, in support or not of other military capabilities. Cyber weapons aim, in accordance with international law, at producing effects against an adversarial computer system to alter availability or data confidentiality."[68]

While the successive documents would give the impression that there have been substantial policy changes over the years, a deeper analysis would show that much of what has been put in the documents is only to formalise the arrangements that have been put in place. To this extent, there is remarkable continuity and sense of purpose on the part of French policy makers. This particularly extends to the personnel that have overseen cybersecurity in France, a subject that was mentioned in the Cybersecurity review, which is, that "experience gained by officials in the field of cybersecurity is optimised throughout their career."[69] Taking the top officials who have served at ANNSI, Cyber Command and DGSE and DGCIS, respectively, Patrick Pailloux, the first Director General of ANNSI, went on to become the Chief Technical Officer of the Directorate General of External Security (DGSE), the French equivalent of the Central Intelligence Agency (CIA). Likewise, then Rear-Admiral Coustellerie was appointed General Officer for Cyber Defense in 2011, a post that he held till 2017 when he was appointed Director General of Information and Communication Systems (DGSIC). The DGSIC was subsequently transformed into the Directorate-General for Digital and Information and Communication (DGNUM) by a government decree in 2018.[70] In addition to adding digital to the nomenclature, the new agency was given expanded powers

---

[68] Francois Delerue et al., "A Close Look at France's New Military Cyber Strategy", *War on the Rocks*, 22 April 2019, available at www.warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/, accessed on 30 June 2019.

[69] n. 57, p. 14.

[70] Dominique Filippone, "La Transformation Numérique Du Ministère des Armées Pilotée Par La DGNUM", *Le Monde Informatique*, 10 July 2018, available at www.lemondeinformatique.fr/actualites/lire-la-transformation-numerique-du-ministere-des-armees-pilotee-par-la-dgnum-72281.html, accessed on 15 March 2019.

to ensure its effective functioning. The main missions of the DGNUM were to orchestrate the digital transformation of the armed forces and to coordinate efficient data flow.[71] The strength of the DGNUM is pegged at 50, comprising both civilian and military personnel. The fact that this organisation is led by a four-star general indicates the level of importance attached to it. [72] In effect, Coustellerie was *de facto* head of the French Cyber Command. [73]

China Strategic Support Force

No study would be complete without an analysis of the reform of the Chinese military, and particularly of the cyber forces. However, such a study has proved to be a difficult task in that much of the reforms are not in the public domain; and even though many articles and other forms of analysis have been made, they are largely speculative and based on both informed and uninformed analysis. However, they serve to bring out the underlying reasons for reform, which are similar to the motivations that have propelled re-organisations in other militaries. These reforms have been ongoing since 2011 and the integration of cyber capabilities, both as a support function as well as a domain area, have been integral to this reform. The specific nature of the restructuring has largely been gleaned out of interpretations by experts on Chinese military and those, in turn, have been based on various inferences drawn from primary and secondary sources, given the secretive nature of the Chinese military. To add to the difficulty in analysis, the reorganisation

---

[71] France, *Legifrance*, Décret n° 2018-532 Du 28 Juin 2018 Fixant L'organisation Du Système D'information Et De Communication De La Défense Et Portant Création De La Direction Générale Du Numérique Et Des Systèmes D'information Et De Communication, 29 June 2018, Articles-2–4.

[72] "Arnaud Coustillière Nommé Vice-Amiral D'Escadre DGSIC Des Armées: Un DSI De Combat", Mag, 3 August 2017, available at www.mag-securs.com/news/id/36052/arnaud-coustilliere-nomme-vice-amiral-d-escadre-dgsic-des-armees-un-dsi-de-combat.aspx, accessed on 15 March 2019.

[73] Raphaël Baldos, "France Commits to Cyberarmy", International.la, 14 December 2016, available at international.la-croix.com/news/france-commits-to-cyberarmy/4363#, accessed on 15 July 2019.

of these units in peacetime is different from the role they are expected to play in wartime, when they are expected to be even more tightly integrated under the moniker of Information Operations Group.

Nonetheless, there are many points that are incontestable: that the need for reform arose from the fact that while Chinese capabilities in new technology-centric domains such as space and cyberspace had improved considerably, the military structure and hierarchies remained the same; that the reforms have been quite substantial despite the fact that the approach undertaken was that of a "bricks, not clay" model, that is, that an organisation would not be built from scratch but existing organisations would be moved around and restructured; and that they seem to have been successful in integrating cyber capabilities across the military.

The People's Liberation Army (PLA) departments relevant to cyber were the Third and Fourth Departments, respectively responsible for technical reconnaissance and offensive cyber operations, and equivalent to US Cyber Command. The Informatization Department was responsible for cyber or information systems defence, comparable to the US National Security Agency (NSA). The Third and Fourth Departments were folded into the Network Systems Department (NSD) of the Strategic Support Force (SSF) created in 2015, which came under the direct control of the Central Military Commission and was not subordinate to the theatre level commands that were created at the same time.[74] In addition, electronic and psychological warfare units were also incorporated into the NSD.[75]

> Before the reorganization, management of these systems was siloed (with each answering only to its parent general department) and differentiated based on source. While the reorganization places all these collection assets under the same organization, the

---

[74] The other branch within the SSF was the Space Systems Department.

[75] John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era", Institute for National Strategic Studies, 2 October 2018, available at ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf, accessed on 23 July 2019.

> advantages inherent to centralization depend heavily on how well the technical systems, data, and organizational procedures that underpin those operations can be integrated. From a purely organizational standpoint, control over these sources of intelligence potentially allows the Strategic Support Force to gain the comprehensive perspective necessary to identify gaps in collection, assess emerging needs, and tailor operations and acquisitions to address shortfalls and new challenges. In short, the sheer breadth of what the SSF can see and hear empowers it to play a decisive role in China's comprehensive domain awareness and national defense far beyond that of any single organization that has come before.[76]

Whilst the moniker Strategic Support Force gives the impression that its main function is support, at the strategic level, its main goal is that of dominating cyberspace and the electromagnetic spectrum and denying its use to its adversaries. This is of paramount importance to a military where the integrity of networks has become as important as logistics and supply chains were to armies of yore. So, providing information support and having the capabilities to conduct information warfare have become two sides of the same coin.

It is evident that the reorganisation has entailed simultaneous restructuring at various levels: (1) with the existing structure of cyber and electronic warfare divisions; (2) plugging in those capabilities along the length and breadth of the PLA; and (3) "maintaining a dual-echelon structure for cyber and EW, with the SSF's cyber force assuming responsibilities for strategic national-level operations, while the services and theater commands continue to be responsible for cyber and EW operations at the operational and tactical levels."[77] By all accounts, this was sought to be achieved by first centralising all the national-level technical collection

---

[76] John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era", Institute for National Strategic Studies, 2 October 2018, p. 37, available at ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf, accessed on 12 January 2019.

[77] Ibid., p. 43.

assets available with the PLA, including space-based, cyber and electronic intelligence collection assets. This potentially allowed the SSF to gain the comprehensive perspective necessary to identify gaps in collection, assess emerging needs, and tailor operations and acquisitions to address shortfalls and new challenges.

The SSF was also integral to the success of the theatre commands and joint operations since it could provide a comprehensive common intelligence picture of the battlespace to the "joint forces within each theater command." "The SSF evolves the PLA's ability to conduct information operations in both peacetime and wartime in a number of ways, namely, integrating these disciplines of information warfare into a unified force, integrating cyber espionage and offense, unifying information warfare campaign planning, and unifying responsibilities for information warfare command and control."[78] On the flip side, it has also been pointed out that centralisation goes against the grain of theatre commands where these commands are supposed to be full self-sufficient units. It would also lead to some amount of tension amongst the competing requirements of espionage, offensive and defensive capabilities and operations.

The case of the Chinese military's capabilities in cyberspace stands out in that it is the only military arm in the cases under study that is actively engaged in cyberconflict against both military and non-military targets. A result of the reorganisation seems to have been that its activities have become much more discreet and that it has become quite careful to cover its tracks.

Whilst each of these militaries have realised the importance of having effective Cyber capabilities as an important component of national power which would also add credibility to their power projection, their efforts to streamline and optimise these capabilities within their militaries has not been without its problems. There have been legacy issues, considering that even though the cyber domain is a new one, its antecedents are present in existing capabilities such as signals and electro-

---

[78] Ibid., p. 41.

magnetic warfare capabilities within the military. The main challenge is that of shifting perspective from considering these capabilities as support capabilities in warfare to being capabilities in their own right which could spell the difference between success and defeat in modern-day cyber-enabled warfare.

Chapter 4

The Use of Technology and Market Regulatory Regimes and Mechanisms with Special Reference to the Wassenaar Arrangement[79]

Technology denial regimes have been used to great effect to restrain countries from acquiring technologies that would augment their national power. In earlier eras, the restraints were on nuclear and space technologies. Treaties such as the Nuclear Non-Proliferation Treaty (NPT), the Missile Technology Control Regime (MTCR) and the Nuclear Suppliers Group denied technologies on the pretext that free availability would lead to insecurity since these technologies were dual use in nature. Since these technologies resided in many countries, the spread was sought to be restricted by harmonising national export control laws through various regimes. Regimes have been defined as informal associations of countries sharing a common interest and operating on a consensus basis without necessarily having the sanctity of an international treaty. The member states agree to voluntarily implement the national export controls in compliance with these regimes, thus giving these regimes the needed authority to interact and cooperate.[80] India was targeted by many of these regimes, particularly

---

[79] The following section incorporates research carried out in the course of undertaking a project for the Ministry of Electronics and Information Technology.

[80] Sameer Patil and Arun Vishwanathan, "India's Approach to Global Export Control Regimes", *Seminar*, Vol. 731, July 2020, available at https://www.india-seminar.com/2020/731/731_sameer_and_arun.htm, accessed on 18 August 2020.

after the nuclear tests of 1998, and several technology transfer and defence cooperation and purchase programmes came to a halt.

In 2012, an attempt was made to adapt the Wassenaar Arrangement, which dealt broadly with dual-use technologies, to include cyber technologies within its ambit. This attempt predated the current technology wars and the focus was on denying non-state actors access to cyber technologies.[81] The relative failure of this attempt highlights the intrinsic issues with adapting these technology denial regimes for cyber.

The Wassenaar Arrangement, the voluntary agreement comprising 41 nations, was set up in 1996 to control the sale and export of conventional arms and goods or technologies having dual use. It was a successor to an earlier arms control regime, the Coordinating Committee for Multilateral Export Controls (COCOM), a grouping of Western countries that targeted exports to the former Soviet Union and its allies. Many of the erstwhile target states, including the Russian Federation, Czech Republic, Hungary, Poland and the Slovak Republic were included in the new grouping. Named as "Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies", it aimed to promote responsibility and transparency in the global arms trade. This was done through the maintenance of two lists, a Munitions List and a list of Dual-Use Goods and Technologies, against which member states provided information on activities, including denial or approval of exports in addition to harmonising laws. Over the years, the controls list has eventually grown to nine categories, including technologies related to information and cyber security.

The Wassenaar Arrangement differed from its predecessor in a number of ways which made it less effective as an arms control mechanism. In the first instance, member states had much more autonomy over

---

[81] Steven E. Miller, "Cyber Threats, Nuclear Analogies? Divergent Trajectories in Adapting to New Dual-Use Technologies STEVEN", in George Perkovich and Ariel Levite (eds), *Understanding Cyber Conflict: 14 Analogies*, Washington D.C.: Georgetown University Press, 2017.

decision making since there was no multilateral oversight mechanism and members did not have the authority to veto the actions of other members, which was a part of the COCOM mechanism. The presence of multiple states with conflicting interests within the grouping without any unifying purpose and competing geopolitical interests also made the grouping less effective than its predecessor.[82]

Background to Inclusion of Information Technologies in Wassenaar List

The United Kingdom (UK) initiated a discussion within the Wassenaar Arrangement in 2012, and in 2013 submitted formal proposals to control the tools (equipment and software) for creating, delivering and controlling "intrusion software" and extracting message content and metadata.[83] Within the European states too there was pressure from human rights activists who were concerned about Internet Protocol (IP) surveillance software being used to locate anti-government activists in authoritarian countries, and to incorporate such provisions in the Wassenaar Arrangement. Intrusion tools, such as Finfisher or the Remote Control Software (RCS) from the Hacking Team, had been found to have been used by oppressive regimes to harass anti-government protestors by tracing their digital footprints. According to human rights activists, these companies operated completely in the dark with no oversight despite the fact that these technologies could be reverse-engineered and proliferated easily once they fell in the hands of terrorists and criminals.[84] In an open letter to the members of the Wassenaar Arrangement, some of the agencies working on human

---

[82] Jukka Ruohonen and Kai K. Kimppa, "Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software, and Ambiguity", *Journal of Information Technology & Politics*, Vol. 16, No. 2, 2019, pp. 169–186, DOI: 10.1080/19331681.2019.1616646.

[83] *United Kingdom Strategic Export Controls Annual Report 2013*, Presented to Parliament pursuant to Section 10 of the Export Control Act 2002 Ordered by the House of Commons to be printed 17 July 2014, p. 7.

[84] Such as Coalition Against Unlawful Surveillance Exports (CAUSE).

rights issues drew the attention of the members towards the rapid proliferation of surveillance technologies accessible to governments having internationally condemned human rights records.[85]

At the 2013 December plenary meeting, participating states agreed to include intrusion malware, exploits and surveillance technologies in the controls list. The participating states of Wassenaar Arrangement agreed to add the following to the list of dual-use goods:

> systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software; technology required for the development of intrusion software; Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefore.[86]

In effect, the updated controls list and the subsequent proposed rule of Bureau of Industry and Security (BIS) of the US Department of Commerce targeted three categories of cyber weapons:

a. "intrusion software/malware"

b. "intrusion exploits", the tools, such as "zero-days", that exploit a vulnerability in a software or system

c. "IP surveillance" products that monitor Internet backbones

---

[85] Namely Amnesty International, Digitale Gesellschaft, FIDH (International Federation for Human Rights), Human Rights Watch, Open Technology Institute, Privacy International.

[86] Department of Commerce, Bureau of Industry and Security, Federal Register, Vol. 80, No. 97, 20 May 2015, p. 28853.

The implementation of controls was to be carried out through national legislation once the participating states agree to maintain the controls.

In order to implement the current Wassenaar Arrangement requirements, the BIS requested for comments on a proposed rule. The rule proposed a license requirement for the export, re-export, or transfer (in-country) of cybersecurity items, identified by the Wassenaar Arrangement, to all destinations, except Canada. The BIS proposal led to an uproar amongst security researchers, security software and testing firms, and even among large software vendors as it had potential implications on legitimate vulnerability research, exploit development, and cyber security products such as commercial penetration testing tools. Many security firms and analysts expressed their concerns pertaining to legitimate business interests and cross-border research collaborations. The proposed legislation stipulated hefty penalties, a 20-year prison sentence and a fine amounting to $1 million for any violation.

Additions to Controls on Software and Technology

The BIS proposed rule first defined "intrusion software", and then listed out the controls, which were applicable on the tools used in the development or production of "intrusion software", but did not apply on "intrusion software" *per se*. The first proposed addition, labelled as "intrusion software"[87] was defined as *software specially designed or modified to avoid detection by "nitoring tools", or to defeat "protective countermeasures" of a computer or network-capable device*. Such software could perform any of the following functions:

a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or

b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions

[87] Ibid., p. 28858.

The changes were ostensibly devised to restrict the sale or distribution of Internet surveillance tools to oppressive regimes. These intrusion tools were originally designed for law enforcement and intelligence agencies by private companies who then proceeded to sell their product to regimes with dubious human rights records.[88] Although, the developers of these tools have denied that their products were sold to repressive regimes, investigations by organisations such as the Citizen Labs at the Munk School of Global Affairs have shown that private companies have exposed the sales of such products to whoever was willing to pay for them. The practice continues to this day as seen in the latest exposure of the breach of the social media messaging programme in May 2019.[89]

Concerns from the Industry

In the run-up to the discussion many security experts warned that such laws would strangle vital security research. Others pointed out that these regulations would severely impact the business fundamentals and competitive ability of legitimate security technology companies due to excessive licensing requirements and delays.[90]

Much of the operations of technology companies are spread across the globe and security product development/research is a collaborative effort, requiring continuous exchange of information and software code for analysis and solution development.

---

88 Kim Zetter, "Why an Arms Control Pact Has Security Experts Up in Arms", 24 June 2015, available at http://www.wired.com/2015/06/arms-control-pact-security-experts-arms/, accessed on 15 October 2017.

89 Hermesauto, "WhatsApp Security Breach Believed to Be Government Surveillance-Linked; 'Select Number of Users' Targeted", *The Straits Times*, 15 May 2019, available at www.straitstimes.com/world/whatsapp-security-breach-may-have-targeted-human-rights-groups, accessed on 13 June 2019.

90 Katie Moussouris, "You Need to Speak Up for Internet Security. Right Now", 16 July 2015, available at http://www.wired.com/2015/07/moussouris-wassenaar-open-comment-period/, accessed on 13 June 2019.

In a comment, Symantec Corporation anticipated that the proposed rule might be detrimental to cyber security industry, by:[91] (1) Restricting access to legitimate cyber security technologies and testing tools across borders, even among security professionals employed by the same company; (2) Curtailing research into system vulnerabilities, as researchers would be hindered from testing networks and sharing technical information across borders; and (3) Limiting cyber threat information sharing and collaboration on security risks, both within security companies and with customers and industry partners.

In other comments, the company behind the penetration testing software Metasploit, an outcome of collaboration between the open source community and Rapid7, which uses multiple types of exploits to test systems, including zero-days, pointed out that the proprietary commercial versions of Metasploit and other penetration testing tools would be subject to license control. Rapid7 anticipated licenses to place a hefty burden on its operations in the form of increased resources to prepare license requests, and to comply with other potential regulatory requirements such as enhanced reporting and pre-shipment notifications. As per a community blog of the firm, the licensing burden would also put Rapid7 and other US companies at a disadvantage when compared to the competitors (who rely on Metasploit Framework) based in the countries outside the Wassenaar Arrangement.[92]

Symantec Corporation, on its company blog, was critical of the proposed rule, stating that "the proposed rule would severely damage

---

[91] *Wassenaar: Cybersecurity and Export Controls, Joint Hearing Before the Subcommittee on Information Technology*, US Government, Homeland Security Digital Library, 12 January 2016, p. 30, available at https://www.hsdl.org/?view&did=806641, accessed on 17 May 2019.

[92] Jen Ellis, "Response to the US Proposal for Implementing the Wassenaar Arrangement Export Controls for Intrusion Software", 12 June 2015, available at https://community.rapid7.com/community/infosec/blog/2015/06/12/response-to-the-us-proposal-for-implementing-the-wassenaar-arrangement-export-controls-for-intrusion-software, accessed on 16 September 2017.

legitimate vulnerability research and security testing worldwide, and thus undermine our ability to protect our own networks and to innovate cybersecurity products and service. The end result is that our customers– businesses, governments and consumers – would be less secure and at greater risk."[93] The issues arise out of the broad language of definitions, affecting a wide array of legitimate cyber security research and network penetration testing. Symantec, as a global security company, has researchers based around the world. The new regulation could require American researchers to obtain a government license in order to have more than a cursory conversation about new security vulnerabilities with their co-workers overseas. In a nutshell, it would handcuff legitimate security companies and researchers while imposing no restrictions on cyber criminals. Ultimately, this would put citizens, businesses and governments at greater risk of cyber-attacks.[94]

Google also noted that multinationals should be able to share information on intrusion software with their engineers globally without the need for licenses, and that where information is fed back to manufacturers in order to fix a vulnerability, there should be license exceptions. Additionally, the proposed rules, as currently written, would have a significant negative impact on the open security research community. The blog post stated that "they would also hamper our ability to defend ourselves, our users, and make the web safer. It would be a disastrous outcome if an export regulation intended to make people more secure resulted in billions of users across the globe becoming persistently less secure."[95]

---

[93] Cheri F. McGuire, "U.S. Commerce Department Controversial Cybersecurity Rule Will Weaken Security Industry and Worldwide Protections", 14 July 2015, available at http://www.symantec.com/connect/blogs/us-commerce-department-controversial-cybersecurity-rule-will-weaken-security-industry-and-worl, accessed on 18 October 2017.

[94] Ibid.

[95] Neil Martin and Tim Willis, "Google, the Wassenaar Arrangement, and the Vulnerability Research", *Google Public Policy Blog*, 20 July 2015, available at http://googlepublicpolicy.blogspot.in/2015/07/google-wassenaar-arrangement-and.html, accessed on 5 February 2018.

A software tool for penetration testing or exploit development is dual use in its characteristics. It may be used to identify vulnerabilities, to reinforce protection measures and avert cyber-attacks. The same tool could also be used for criminal or other nefarious purposes. Such a pervasive licensing regimen would severely impact the organisations using these tools or software for statutory purposes, in the form of significant alterations to the internal processes and compliance programmes as well as additional export licensing requirements.[96]

Concerns from Security Research

Security researchers have opined in various articles that the definitions are extremely broad. In technical terms, intrusion software is "modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions." According to James Gannon, Director and Principal of Cyber Invasion Ltd., this definition encompasses methods and tools that are common to software engineering, posing a genuine risk that these controls will hamper the ability of researchers. The techniques defined are used across many platforms, from anti-virus software to operating systems, from malware analysis to games development.[97]

The computer industry makes extensive use of bug bounty programs, which offer incentives for security researchers to participate and find vulnerabilities during exercises. The vulnerabilities are disclosed and there upon patched by the application developers. Katie Moussouris,

---

[96] Sergey Bratus, Michael Locasto and Anna Shubina, "Why Wassenaar Arrangement's Definitions of 'Intrusion Software' and 'Controlled Items' Put Security Research and Defense At Risk", 23 July 2014, p. 2, available at https://www.usenix.org/system/files/login/articles/wassenaar.pdf, accessed on 16 October 2017.

[97] James Gannon, "Wassenaar: Turning Arms Control Into Software Control", *Internet Governance Project*, 25 May 2015, available at http://www.internetgovernance.org/2015/05/25/wassenaar-turning-arms-control-into-software-control/, accessed on 14 July 2017.

chief policy officer of HackerOne,[98] expressed her concerns that the government has not understood the nuances of security research and vulnerability disclosures. The international security research community works in cohesion, cutting across borders, and she has been sceptical whether researchers would continue to collaborate.[99]

Noted security researcher Halvar Flake articulated that security research across international borders would be stifled. This "balkanisation" or division of security researchers by country—those covered by Wassenaar and those where it is not applied—would slow fundamental advancements in computer security, hindering breakthroughs in defence.[100]

Many experts speculated that the end result of such actions would be to push security research into the underground black market, where software and exploits would be traded illegally instead of openly with the companies. If the vulnerabilities and exploits were traded in black market,[101] they could easily be picked by criminal enterprises instead of being reported and fixed.

It was quite evident from the documents of proposed rule, that the controls were not aimed at malware or rootkits that are actually responsible for intrusion. Rather, the controls would be applicable on

---

98 Hacker One runs bug bounty programs for some of the computer industry's biggest names such as Yahoo, Twitter, Square and Dropbox.

99 Joe Uchill, "Industry Warns Proposed Arms Export Rule will Thwart Basic Cyberdefenses", *The Christian Science Monitor*, 26 June 2015, available at http://www.csmonitor.com/World/Passcode/2015/0626/Industry-warns-proposed-arms-export-rule-will-thwart-basic-cyberdefenses, accessed on 16 October 2018.

100 Brewster, Thomas. "Why the World's Top Security Pros Are Furious about Exploit Export Rules." Forbes Magazine, 27 May 2015, www.forbes.com/sites/thomasbrewster/2015/05/26/security-pro-fury-on-exploit-export-rules . accessed on 23 May 2017.

101 Lillian Ablon, Martin C. Libicki and Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data", RAND Corporation, 2014, available at http://www.rand.org/pubs/research_reports/RR610.html, accessed on 1 March 2017.

the software or platforms that are used to develop, deliver and command or control the intrusion software or malware. These controls explicitly define intrusion software in terms of its capability to extract or modify data or modify the standard execution path of software, malware that can damage or destroy systems or infrastructure is excluded. All applications need updates, and these updates are normally performed automatically, without the user's intervention. The proposed rule excludes auto-update functionality and anti-virus tools from Export Administration Regulations (EAR), in addition to port scanners, vulnerability scanners, packet sniffers, protocol analysers and some of the penetration testing tools. In the present form, the proposed rule has made an effort to ensure that Export Administration Regulations (EAR) does not hamper security research. Therefore, exchange of technical information for the purpose of publishing or releasing at open conferences has been wisely excluded. The controls do not apply to technology or software available in the public domain.

To summarise the arguments of those affected by the proposed rules, malware analysis and patching is a dynamic and challenging process with anti-virus companies registering as much as 3,65,000 new malware a day and over 24 million in a year.[102] These malwares are analysed at different places according to the availability of the expertise. Not only would the envisaged export control regulations put a hefty burden on cyber security solutions companies, but the proposed rule would also interfere with the seamless transnational nature of the process. Obtaining an export license is a time-consuming process and an expected surge would lead to delays in development and delivery of cybersecurity solutions. The delays would render the users vulnerable to attacks in the meantime before the fix is delivered and deployed. Additionally, this might lead to collateral costs if the customers are compromised in the meantime. The proposed rule would restrict individual security researchers, small security companies who have potential to disrupt security solutions, large firms which employ foreign nationals and firms

---

[102] Josh Fruhlinger, "Top Cybersecurity Facts, Figures and Statistics for 2020", *CSO Online*, CSO, 9 March 2020, available at www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html, accessed on 10 July 2020.

which rely on or leverage open source security research in their proprietary products. The restriction put on them, in terms of exchange of ideas, code or information might impact the fabric of security research, collaboration and corroboration on vulnerability research. Licensing requirements would further add to delays and costs.

As a result of the opposition, the rules were never notified in the United States. However, the cross-domain issues raised during the process are still relevant and highlight the difficulties of using technology denial as an instrument of coercion in cyberspace.

At the time the proposed rules were announced, India was not yet a member of the Wassenaar Arrangement.[103] There was considerable disquiet from the private sector as well as from the government as to how these rules would impact export of technology to India, which was a vast market for security software and highly dependent on imports of such software.[104] The proposed rules seemed to make even something as commonplace as auto-updating of browsers illegal. A preliminary reading of these rules indicated that the source code of sensitive products should be examined by the relevant authorities prior to export. As early as June 2014, an inter-ministerial panel of the Indian government was formed to study the impact of the new rules on procurement of software and cybersecurity products. The remit of the committee included negotiating with six countries that were part of the Arrangement and held most of the intellectual property on cyber technologies, including the US, the UK, Israel, Germany, France and Canada.[105]

---

[103] Martand Jha, "India and the Wassenaar Arrangement", *The Mint*, 3 February 2018, available at www.livemint.com/Sundayapp/AETSo9p0H9Dii7ou9WRvrO/India-and-the-Wassenaar-Arrangement.html, accessed on 4 March 2019.

[104] Thomas K. Thomas, "New Export Control Law Could Threaten India's Cyber Security Programme", *The Hindu Business Line*, 19 June 2014, available at www.thehindubusinessline.com/info-tech/new-export-control-law-could-threaten-indias-cyber-security-programme/article20802054.ece, accessed on 14 April 2017.

[105] Ibid.

In their seminal work on international relations, Palmer and Perkins noted that technological prowess was an essential element of national power and states would employ both technological and economic access as a means of denying other powers a means to increase their national power. Inasmuch as multilateral technology control regimes were relatively successfully deployed earlier to deny conventional and nuclear technology to competitor powers and non-state actors, the same has been sought to be replicated for cyber technologies, in the above case, through the mechanism of the Wassenaar Arrangement. This particular attempt failed because there were strong commercial constituencies in multiple countries that opposed to the proposed rules. That notwithstanding, most of the technologies that were sought to be brought within its ambit were largely available off the shelf; it is the next generation of cyber technologies incorporating other advanced technologies and innovations such as quantum computing and artificial intelligence that will again result in a technology gap and renewed efforts to prevent the proliferation of these technologies, as was seen in earlier times.[106] There are still a large number of variables that would decide whether an arms control/technology denial approach would succeed in cyberspace.

---

[106] Amitav Mallik, "Technology and Security in the 21st Century: A Demand-side Perspective", SIPRI Research Report No. 20, Oxford University Press, 2004, pp. 117–121.

Chapter 5

Enhancing Cyber Power Through Regional Cooperation

The role of regional organisations in cyber confidence building can range from: (1) bringing together states that have difficult relations; (2) providing a forum for neighbours to talk and resolve grievances; (3) reducing suspicions among neighbouring states; and (4) establishing mechanisms to address actual disputes. Successive United Nations Group of Governmental Experts (UN GGE) reports have highlighted the role of these organisations in "increasing transparency, engage in trust building and pursuing risk reduction". Measures suggested to increase transparency have included exchanging information on domestic structures and institutions, and national cyber security strategies. Trust building measures include sharing of viewpoints on international cyber conflicts, contact points and structures and establishing communication channels for crisis situations. Risk reduction could be achieved by establishing national CERTs and conducting joint CERT exercises.

The United Nations and Regional Organisations

The absence of a central regulator and the distributed nature of cyberspace has been touted as one of the reasons for its success, and unprecedented expansion in a relatively short span of time. These same characteristics have brought about increasing instability and insecurity, exacerbated by malicious actors. The United Nations has been at the forefront of attempts to establish norms and conventions in cyberspace, but these efforts have been stymied by geopolitical manoeuvring. That notwithstanding, regional organisations have been identified as the vehicles through which the recommendations and resolutions made at the highest level may be implemented.

The United Nations established Group of Governmental Experts has mainly been concerned with norms, confidence-building and capacity-building measures and their implementation. These GGEs, even with such a relatively limited focus, were unable to forge consensus, leading

to a collapse of the process in 2017. A new GGE was constituted to continue exploring these same issues within a time span of three years. Along with it, an open-ended working group was established, which was not limited to just member states, but also included participation by "business, non-governmental organizations and the academic community via intersessional consultative meetings." Whilst the UNGGE resolution was sponsored by the Western countries, the Open-Ended Working Group (OEWG) resolution's primary backer was Russia, reflecting the geopolitical schisms that have developed around the governance of cyberspace. In the vote on the respective resolutions, the Western countries voted against the Russian resolution. A total of 109 states voted in favour of the resolution, with 46 voting against and 14 abstaining. The US resolution on the UNGGE had 139 in favour, 11 against and 16 abstentions. India voted for both resolutions while Pakistan was one of the co-sponsors of the Russia and China backed resolutions and abstained from voting on the US-backed resolution.

That aside, the draft resolution A/C.1/73/L.37 of 18 October 2018 on "Advancing responsible State behaviour in cyberspace in the context of international security" highlighted the importance of regional organisations, requesting the

> Office for Disarmament Affairs of the Secretariat, through existing resources and voluntary contributions, on behalf of the members of the group of governmental experts, to collaborate with relevant regional organizations, such as the African Union, the European Union, the Organization of American States, the Organization for Security and Cooperation in Europe and the Regional Forum of the Association of Southeast Asian Nations, to convene a series of consultations to share views on the issues within the mandate of the group in advance of its sessions…[107]

Given the importance of the sub-regional organisations in the scheme of things, it is not surprising that major powers try to have some

---

[107] United Nations, Agenda Item 93, A/73/505, Developments in the field of information and telecommunications in the context of international security, Report of the First Committee A/73/505, 19 November 2018.

influence even in those sub-regional fora outside their respective regions, with the competing powers trying to make an entry in the form of observers or providers of expertise and training.

A Case Study of ASEAN

A case in point is the Southeast Asian region—the Association of Southeast Asian Nations (ASEAN) has been actively promoting the concept of cybersecurity among its member states with the active participation and support of the United States.[108] Its role in ensuring peace and stability in cyberspace in Asia goes back to its existing role as a balancer in great power politics in the Asia–Pacific.[109] However, it is the ASEAN Regional Forum (ARF) that has become the more relevant forum to deal with cybersecurity since its dialogue partners also include Russia, China, the United States and India.[110]

The ASEAN Regional Forum is the premier regional forum for discussing cybersecurity issues in the Asia–Pacific region and it brings together a diverse set of countries. That diversity also extends to cyberspace. While some countries have advanced capabilities and capacities as well as comprehensive policy mechanisms, other countries have only just started the process. The vast gap in capacities and capabilities of states institutions, technical organisations and the private sector, as well as policy mechanisms and relevant legislation is a major obstacle to intra-regional cooperation. Part of the problem is also the

---

[108] Cybercrime was placed on the agenda of the ASEAN ministerial meetings as early as 2001. Ralf Emmers, The Securitization of Transnational Crime in ASEAN, Working Paper, Institute of Defence and Strategic Studies, Singapore 2002, p. 14.

[109] Caitríona H. Heinl, *Regional Cyber Security: Moving Towards a Resilient ASEAN Cyber Security Regime*, S. Rajaratnam School of International Studies, Singapore, 2013, p. 33.

[110] In total, the ARF consists of 27 countries including the 10 ASEAN member states (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam); the 10 ASEAN dialogue partners (Australia, Canada, China, the EU, India, Japan, New Zealand, ROK, Russia and the United States) as well as the Democratic People's Republic of Korea (DPRK), Mongolia, Pakistan, Timor-Leste, Bangladesh and Sri Lanka.

fact that no fora exist for cross-sector discussion on cyber issues apart from fora such as ASEAN and ARF where cyber security is usually part of a wider agenda. Even dedicated Track 2 initiatives are far and few between. So, capacity building has to be and is a collective enterprise.

Background

The ARF organised a series of seminars on cyberterrorism between 2004 and 2007, but some member countries were uncomfortable with the notion of cyberterrorism. The "Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space" was released at the end of the 13th ASEAN Regional Forum at Kuala Lumpur in 2006. It urged member countries to enact laws and adopt policy frameworks on cybercrime and cybersecurity. In 2012, the ARF again kickstarted its programme on cybersecurity with the adoption of an ARF Statement on Cooperation in Ensuring Cyber Security. The foreign ministers present also agreed to adopt a work plan on cybersecurity.[111]

Among the major points in the declaration were the following:

- Promote further consideration of strategies to address threats emerging in this field consistent with international law and its basic principles.
- Promote dialogue on confidence building, stability, and risk reduction measures to address the implications of ARF participants' use of ICTs, including exchange of views on the potential use of ICTs in conflict.
- Encourage and enhance cooperation in bringing about culture of cyber security.
- Develop an ARF work plan on security in the use of ICTs, focused on practical cooperation on confidence-building

---

[111] ASEAN Regional Forum Statement by the Ministers of Foreign Affairs on Cooperation In Ensuring Cyber Security, 12 July 2012, p .2, available at https://ccdcoe.org/sites/default/files/documents/ASEAN-120712-ARFStatementCS.pdf, accessed on 14 August 2017.

measures, which could set out corresponding goals and timeframes for their implementation.

- Review a possibility to elaborate common terms and definitions relevant to the sphere of the use of ICTs.

The ARF has had two objectives when it comes to cybersecurity: (1) Confidence-building and transparency measures—develop confidence-building and other transparency measures to reduce the risk of misperception, escalation and conflict, and consideration of strategies to address threats emerging in this field consistent with international law and its basic principles, (2) Capacity building—develop the capacity of governments to secure their ICT systems and to protect their critical infrastructure, and encourage and enhance cooperation in bringing about a culture of cybersecurity. Being relatively non-controversial, a certain amount of activity has taken place by way of workshops and meetings.

The first workshop that took place under ARF auspices was the "Workshop on Measures to Enhance Cyber Security—Legal and Cultural Aspects" which was hosted by China in September 2013. This workshop had sessions on national and regional practices on cyber security, capacity building to strengthen cybersecurity, cultural dimensions in cyberspace, regional cooperation in combating cybercrimes, and the role of states in cyberspace.[112] The difference among the participants is reflected in the co-chair's summary as well as in reports on the event.[113]

In March 2014, a second workshop on Cyber Confidence Building Measures, co-sponsored by Australia was held in Malaysia on "Confidence building measures in Cyberspace". The workshop was constructed around five modules: (1) The Nature, Importance and

---

[112] ASEAN Regional Forum. Co-Chairs' Summary Report of the ARF Workshop on Measures to Enhance Cyber Security—Legal and Cultural Aspects, 2 September 2013, N.p., n.d. Web. 13 December 2015.

[113] Tobias Feakin, "ARF, and How to Change the Tune of the Cyber Debate", *The Strategist*, Australian Strategic Policy Institute, 14 October 2013, available at http://www.aspistrategist.org.au/arf-and-how-to-change-the-tune-of-the-cyber-debate/, accessed on 15 November 2016.

Need for Cyber Confidence-Building and Transparency Measures; (2) National Cyber Security Architectures— Which Points of Contact are Vital?; (3) Two-Part Desktop Simulation; (4) The Role and Importance of Points of Contact; and (5) Building a Regional Network of Contacts. This workshop was designed to be closely aligned with the recommendations of the 2013 UN GGE report.

More than 40 per cent of the global Internet population resides in the Asia–Pacific region amounting to 644 million users. National interest was forcing states to become actors in cyberspace. Hence, there was an urgent need to have baseline measures such as cyber points of contact, and awareness of each other's cybersecurity structures in place to minimise the risk of misunderstandings and misperceptions that could have potentially catastrophic consequences. Recognition of this had led to two important agreements in the 2013 UN GGE: (1) existing international law applies in cyberspace; (2) voluntary Confidence-Building Measures (CBMs) can play an important role in advancing peace and security. In line with this, the aims of the ARF dialogue were to work on confidence building and preventive diplomacy, eventually paving the way for a conflict resolution capacity.

The United States' perspective is that while networks are not owned or controlled by states, they have an important and unique role to maintain international peace and security. Rather than trying to do this through regulation, states should work with other stakeholders to make sure this important resource remains available to all. With increasing dependence on these networks and threats to critical networks and cyber-enabled infrastructure on the rise, the solution lay in trans-national cooperation and focus on norms and capacity building.

The Chinese perspective is that China was all in favour of confidence-building measures, but it should be developed on "a voluntary basis, taking into account different country, different situations and time as well as in a phased and incremental process". China has been playing a constructive role through CBMs; firstly, China had launched bilateral dialogues and consultations and constructively participated in the work of UN GGE and regional cooperative frameworks. Secondly, China had established extensive international cooperation among CERTs and law enforcement agencies. Thirdly, China and Russia along with other Shanghai Cooperation Organization members submitted to the United

Nations General Assembly an "International Code of Conduct for Information Security" in 2011 as an input into international deliberation on international norms and rules.

An examination of the initial and final drafts of the ARF workplan shows the delicate path countries of the region have to tread in trying to forge a workable plan while keeping the sensitivities of various countries in mind.[114]

The objectives of the work plan are to:

~~(a)~~ (a) promote transparency and develop confidence building measures to enhance the understanding of ARF Participating Countries in the ICT environment with a view to reducing the risk of misperception, miscalculation and escalation~~;~~

~~1~~

~~DRAFT~~

~~19 March 2014~~

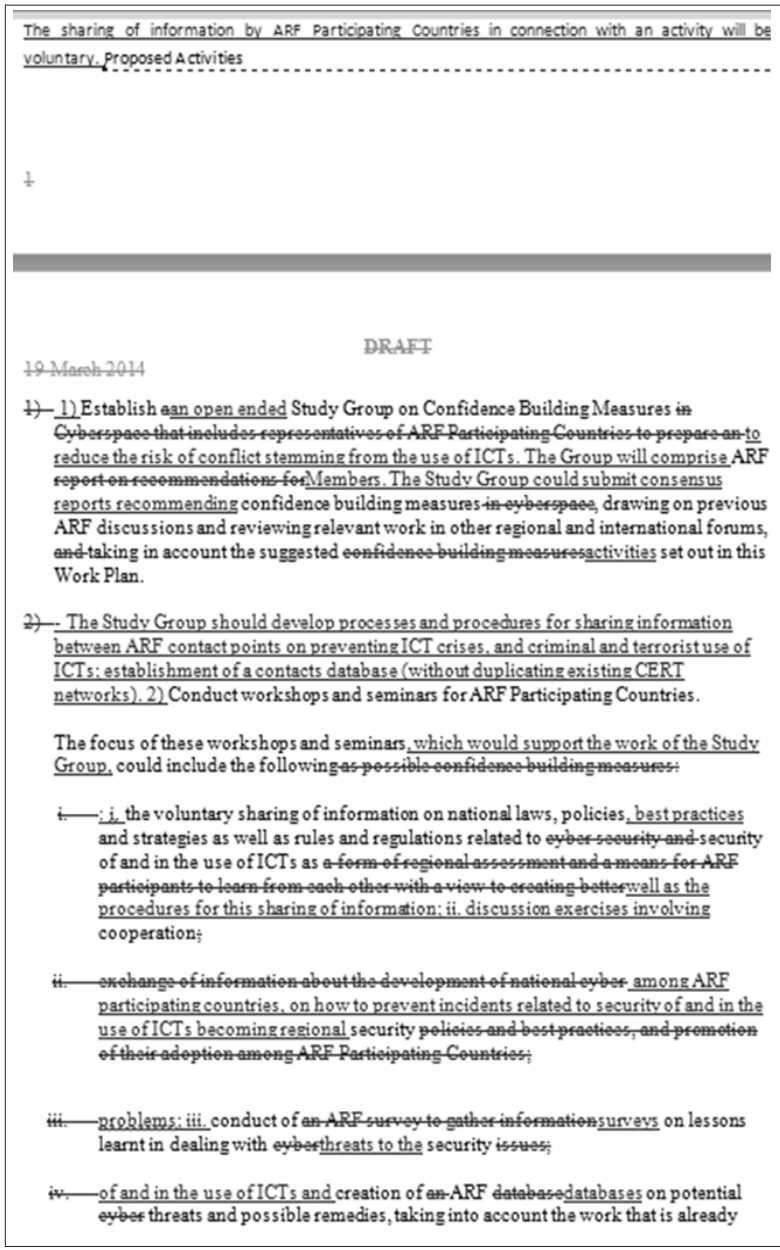
~~(b)~~ of tension leading to conflict; (b) raise awareness on threats related to the security of and in the use of ICTs;

~~(c)~~ (c) enhance practical cooperation between ARF Participating Countries ~~towards the development of a resilient government ICT environment and~~ to protect ~~cyber~~ICT-enabled critical infrastructure~~; and~~

~~(d)~~ with the view to also developing resilient government ICT environments; and (d) Improve cooperation including develop regional capacity to respond to criminal and terrorist use of ICTs through improved coordination and coordinated response.

[114] The final version of the workplan is available at https://aseanregionalforum.asean.org/wp-content/uploads/2018/07/ARF-Work-Plan-on-Security-of-and-in-the-Use-of-Information-and-Communications-Technologies.pdf

Much of the text has been watered down and the tone changed from active to passive. Additional text included makes clear that all activities are voluntary.



The sharing of information by ARF Participating Countries in connection with an activity will be voluntary. Proposed Activities

1

DRAFT

19 March 2014

1) 1) Establish aan open ended Study Group on Confidence Building Measures in Cyberspace that includes representatives of ARF Participating Countries to prepare an to reduce the risk of conflict stemming from the use of ICTs. The Group will comprise ARF report on recommendations for Members. The Study Group could submit consensus reports recommending confidence building measures in cyberspace, drawing on previous ARF discussions and reviewing relevant work in other regional and international forums, and taking in account the suggested confidence building measures activities set out in this Work Plan.

2) . The Study Group should develop processes and procedures for sharing information between ARF contact points on preventing ICT crises, and criminal and terrorist use of ICTs; establishment of a contacts database (without duplicating existing CERT networks). 2) Conduct workshops and seminars for ARF Participating Countries.

The focus of these workshops and seminars, which would support the work of the Study Group, could include the following as possible confidence building measures:

i. ; i. the voluntary sharing of information on national laws, policies, best practices and strategies as well as rules and regulations related to cyber security and security of and in the use of ICTs as a form of regional assessment and a means for ARF participants to learn from each other with a view to creating betterwell as the procedures for this sharing of information; ii. discussion exercises involving cooperation;

ii. exchange of information about the development of national cyber among ARF participating countries, on how to prevent incidents related to security of and in the use of ICTs becoming regional security policies and best practices, and promotion of their adoption among ARF Participating Countries;

iii. problems; iii. conduct of an ARF survey to gather information surveys on lessons learnt in dealing with cyberthreats to the security issues;

iv. of and in the use of ICTs and creation of an ARF databasedatabases on potential cyber threats and possible remedies, taking into account the work that is already

The removal of terms such as confidence-building measures and replacement of "cybersecurity" with "ICT" would also indicate that some countries have prevailed in their preferences and objections towards such terms.

In the final analysis, organising regional cooperation comes with a series of challenges related to competition between the larger powers in the group and vested interests and different capacity levels. In the larger ASEAN and ARF ecosystem, while some countries such as Japan and Korea have advanced capabilities and capacities, other countries such as Laos has only just embarked on establishing a CERT. The Organisation for Security and Co-opeartion in Europe (OSCE), the nodal organisation of the Western countries, along with regional participants such as Australia and New Zealand, in this particular instance, played an important behind-the-scene role in directing the agenda.

Lessons for South Asia

Scope for a regional association in South Asia

Virtually every region has a regional organisation that has taken on the onus of discussing cybersecurity, with the solitary exception of South Asia. This affects the ability of countries in the region to contribute to the global conversation on cybersecurity. And as the leading power in the region, it also deprives India of a forum to strengthen the security of South Asia which is home to a quarter of people online. In cybersecurity, more than elsewhere, malicious actors are looking for vulnerabilities and attack points in networks, which are more likely to be connected on a regional level. Thus, a vulnerable network in the region is almost akin to an insider threat which can impact all the networks in the region. At a more granular level, the legal and policy framework that have been put in place dictate the extent to which respective law enforcement agencies can cooperate to prosecute cybercriminals. Regional organisations can also help in facilitating database and information sharing, both essential to catching cyber criminals who are oftentimes working cross-border.

As far as providing solution at a regional level is concerned, South Asia is particularly affected since a regional organisation such as the South

Asian Association of Regional Cooperation (SAARC) is finding it difficult to forge cooperation and consensus on even traditional security issues and it has not yet taken up cybersecurity as an agenda item. As an economic and geopolitical organisation, SAARC can play a pivotal role in capacity building as well coordinating cybersecurity efforts of all members facing non-traditional security threats from non-state actors to both their populace and businesses, in form of terrorism, cybercrime etc.

The BIMSTEC Initiative

However, given the failure of SAARC to fulfil the function of being a sub-regional organisation dealing with cybersecurity issues in the region, the other regional organisation that could step into the breach is the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC). The BIMSTEC was formed in 1997 and comprises all the countries in SAARC barring Afghanistan, Pakistan and the Maldives, but including Thailand and Myanmar. Cybersecurity came on the radar of the BIMSTEC states at the meeting of National Security Chiefs of Member States on Information and Intelligence Sharing in 2017 where they noted that emerging trends in cyberspace have security implications, and decided to establish a Joint Forum to strengthen cyber security among the BIMSTEC member states.[115] India proposed a three-day workshop on cybersecurity for the BIMSTEC member states at the second meeting of the BIMSTEC National Security Chiefs, held in August 2018. At the workshop conducted in December 2018, the participants adopted a Roadmap for BIMSTEC Cyber Security Cooperation. The salient points of the roadmap were:

- Develop mechanisms for sharing of information on cyber threats, malware and cyber incidents.

---

[115] "MEA | Statements: Press Releases". First meeting of the BIMSTEC National Security Chiefs (21 March 2017), Ministry of External Affairs, Government of India, available at www.mea.gov.in/press-releases.htm?dtl%2F28193%2FFirst_meeting_of_the_BIMSTEC_National_Security_Chiefs, 21_March_2017, accessed on 13 October 2018.

- Identify areas of cooperation in various aspects of cybersecurity, including capacity building.
- Establish a BIMSTEC CERT-to-CERT cooperation mechanism.
- Share experiences and best practices for the protection of critical information infrastructure.
- Strengthen law enforcement cooperation to address cybercrime, cyber terrorism and cybersecurity.
- Develop a BIMSTEC perspective on international cyber issues such as Internet governance, cyber norms, data sovereignty, data protection, privacy.
- Work together on developing voluntary norms of responsible state behaviour in cyberspace, to ensure an open, accessible, secure, stable, peaceful and equitable ICT environment.
- Encourage cooperation among stakeholders including government, private sector, civil society and academia for exchange of expertise, joint research, workshops and seminars.
- Promote capacity building and skill development in the areas of cybersecurity.
- Hold BIMSTEC Cyber Security Workshop annually on voluntary and rotational basis, as a regional forum to discuss various aspects of cybersecurity cooperation.

Whilst the BIMSTEC effort is a commendable one, it is still at a nascent stage, and would require sustained push to make it an ongoing concern. Thailand and Myanmar highlight one of the main issues with forging regional cooperation in cybersecurity: the wide gap between member states. Thailand is among the more advanced states even within ASEAN. As one of the erstwhile tiger economies of Asia, Thailand has a relatively high number of Internet users in proportion to the population at 53 per cent. Thailand has over a dozen undersea cables, with the first one connected in 1997. The official CERT, THAICERT was set up in 2000 and comes under the Electronic Transactions Development Agency (ETDA), which is an agency of the Ministry of Digital Economy

and Society.[116] The Ministry of Information and Communication Technology, established in 2002, was dissolved and replaced with the Ministry of Digital Economy and Society in 2016. A National Cybersecurity Strategy 2017–2021 plan has been put in motion, with the objective of securing Thailand's cyberspace through the promulgation of various acts, including a Cybersecurity Act, and the creation of agencies, including a National Cyber Security Committee to be headed by the Prime Minister.[117]

Myanmar deregulated its telecom and communications sector only in 2013; hitherto, it had been a monopoly of the government-owned Myanmar Posts and Telecommunications (MPT). Within a few years, and partly because Myanmar was able to leapfrog technologies, Internet penetration has reached 35 per cent, and has accelerated even more after the introduction of 4G services in 2018.

On the governance side, a National Cyber Security Steering Committee was instituted in 2011 with six working committees on issues from research development and training on cybersecurity to international cooperation. Much of the focus remains on cybercrime with registered cases going up from two in 2013 to 448 in 2018. Cyberlaw legislation was due to be placed before the parliament.[118] After the military took over, there have been attempts to amend the draft cybersecurity laws.Myanmar has greatly benefitted from cooperation within the ASEAN, through mechanisms and fora such as ASEANAOPOL (the National Police Organisation for the Association of Southeast Asian

---

[116] "THAICERT-About Us", ThaiCERT, available at www.thaicert.or.th/about-en.html, accessed on 11 June 2017.

[117] "Thailand Passes Controversial Cybersecurity Law That Could Enable Government Surveillance", *TechCrunch*, 28 February 2019, available at techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/, accessed on 16 March 2019.

[118] Aung Thiha Irrawaddy, "With Myanmar's Internet Expansion, Cybercrimes Soar", *The Irrawaddy*, 10 July 2019, available at www.irrawaddy.com/news/burma/myanmars-internet-expansion-cybercrimes-soar.html, accessed on 10 August 2019.

Nations), the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), Senior Officials Meeting on Transnational Crime (SOMTC) and the ASEAN Regional Forum (ARF).

A cyber maturity assessment of the countries of the South Asian region

The geopolitical aspects notwithstanding, a cyber maturity assessment would give a fair idea of where countries in the South Asian region are placed in terms of their cybersecurity, and the capabilities and capacities they bring to the table.

Pakistan

In 2013, there were a reported 30 million Internet users in Pakistan, amounting to about 10 per cent of the population.[119] By 2019, the figure had increased to 44 million. Pakistan has access through the SEA–ME–WE-3 and SEA–ME–WE-4 submarine cable systems, the TWA-1 telecommunications cable linking the United Arab Emirates, Oman and Pakistan, as well as three Intelsat satellite earth stations.

In terms of cybersecurity, the country faces the same problems faced by other developing countries, including lack of capabilities and capacities in technical, legal, law enforcement and other arenas. However, there is insufficient legislation in place to protect Pakistanis against what they are most likely to face by way of cybercrimes. The earliest piece of legislation was the Electronic Transactions Ordinance 2002 which largely dealt with the data protection. The Prevention of Electronic Crimes Ordinance (PECO) was promulgated in 2007 and expired in 2009. It dealt with electronic crimes including cyber terrorism, data damage, electronic fraud, electronic forgery, unauthorised access to code, cyber stalking and cyber spamming. When it was sought to be converted to a law, it was blocked by legislators who felt its provisions

---

[119] "30m Internet Users in Pakistan, Half on Mobile", *The Express Tribune*, 24 June 2013, available at http://tribune.com.pk/story/567649/30m-internet-users-in-pakistan-half-on-mobile-report/, accessed on 13 April 2016. InternetworldStats put the figure at 14 million in December 2014.

impinged on fundamental rights.[120] The Prevention of Electronic Crimes Act passed in 2016 contained provisions for dealing with various types of crimes ranging from pornography to terrorism.[121] One of the more unusual provision was that contained in Chapter 7, Subsection 46(2) which provided for intelligence officials to be a part of one or more CERTs to be set up.[122] The Act , even while in the bill stage was severely criticised for undermining individual rights, even at the international level.[123]

The events leading up to the passing of the bill were also shrouded in controversy. In January 2015, the Government of Pakistan drafted the Prevention of Electronic Crimes Bill (PECB). Ostensibly the PECB was written to address new digital issues, such as cyberstalking, forgery, and online harassment. The PECB was introduced in the same period as the Government of Pakistan established its National Action Plan (NAP), a comprehensive state-level project to combat terrorism after armed men linked to the Taliban, attacked an Army-run school in the city of Peshawar, killing 145 people, 132 of whom were children. The PECB became part of the NAP: a political product intended to make control of political expression an official role of the government. Section 34 of the PECB, for example, gives the Pakistan Telecommunication Authority (PTA) powers to block objectionable content and websites, with very vague, unclear ideas as to what constitutes "objectionable". If the PTA determine that it is "necessary

---

120 "Investigators Suffering from Absence of Law", *The Express Tribune*, 24 March 2011, available at http://tribune.com.pk/story/136794/investigators-suffering-from-absence-of-law/, accessed on 25 November 2015.

121 Pakistan, National Assembly, *The Prevention of Electronic Crimes Act, 2016*, available at http://www.na.gov.pk/uploads/documents/1472635250_246.pdf, accessed on 19 July 2017.

122 Ibid., p. 25.

123 "UN Expert Urges Pakistan to Ensure Protection of Freedom of Expression in Draft Cybercrime Bill", Office of High Commissioner for Human Rights, United Nations, 14 December 2015, available at www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16879&LangID=E, accessed on 17 September 2017.

in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign states, public order, decency or morality," then the authorities can censor it. On 17 September 2015, however, the Standing Committee decided to approve the draft and send it on its way to the National Assembly. Actually, to be more precise: copies of the draft were not given by the drafters to other committee members. When they objected and stressed that the drafted bill could not be approved without review, they were overruled by the committee chair, who said that as he had seen the draft, that would be sufficient to pass it onto the National Assembly.

Similar was the process with establishing a National Cyber Security Strategy in 2013. The Pakistan Senate began an initiative to legislate on a National Cyber Security Strategy in 2013 following the Snowden revelations, which indicated that Pakistan had been a major target of the US National Security Agency. The initiative was led by the Chairman of the Senate Defence Committee who also announced a Task Force on Cybersecurity Policy with the following objectives:

(1) Produce a Cyber Security Bill to Provide Framework for Preservation, Protection and Promotion of Pakistan's Cybersecurity.

(2) Establishment of Pakistan Computer Emergency Response Team (PakCERT).

(3) Establishment of a cybersecurity task force in collaboration with the Ministry of Defence, Ministry of Information Technology, Ministry of Interior, Ministry of Foreign Affairs, Ministry of Information, Security Organizations and Security Professionals to formulate the National Cyber Security Strategy.

(4) Establishment of an Inter Services Cyber Command under the Office of the Chairman Joint Chiefs of Staff Committee to coordinate cybersecurity and cyber defence for the armed forces.

(5) Initiating talks within the auspices of SAARC to establish acceptable regional norms of cyber behaviour so that members do not engage in cyber-warfare against each other.

(6) Concluding an agreement with India not to engage in cyber-warfare patterned on the agreement not to attack nuclear installations.

(7) Organising a special media workshop to promote awareness among the public and educate opinion leaders on the issue of cybersecurity and educate opinion leaders on the issue of cybersecurity.[124]

A secondary objective was to create a National Cybersecurity Council. A bill to that effect was introduced in the Senate on 14 April 2014. The members of the council comprised of stakeholders from the government as well as the private sector, 21 and 11 respectively, to number 32 in total.[125] The Senate was informed on November 2014 that the bill had been rejected by the government following consultations with "all the stakeholders including the Inter-Services Intelligence (ISI)." In a written reply to the Senate, the specific objections given were: (1) "It may not adequately address the issue of cyber security and falls short of addressing the key problems linked with cyber security – personal data protection and unauthorised interceptions"; (2) The bill does not even provide guidance to the proposed council in light of which the council may devise policy to ensure that the fundamental rights of citizens of Pakistan are protected; and (3) The bill also does not require the operators of critical information systems in government, financial, e-commerce, social networks, etc. sectors to report major security incidents on their core services. [It] also falls short of imposing a positive obligation on the operators in the said sectors to adopt risk management practices.[126]

---

[124] Tughral Yamin, "Developing Information-Space Confidence Building Measures (CBMs) between India and Pakistan", Issue Brief: *Sandia Report*, June 2014, p. 94.

[125] Pakistan Senate, *BILL to Provide for the Establishment of a National Cyber Security Council*, Islamabad, 14 April 2014, available at http://www.senate.gov.pk/uploads/documents/1397624997_197.pdf, accessed on 26 November 2015.

[126] "Curbing Cybercrimes: Ministry Rejects Cyber Security Council Bill", *The Express Tribune*, 12 November 2014, available at http://tribune.com.pk/story/789626/curbing-cybercrimes-ministry-rejects-cyber-security-council-bill/, accessed on 25 November 2015.

These efforts notwithstanding, there were regular news reports related to the Snowden leaks about the interception of Pakistani Internet traffic by Western intelligence agencies. These ranged from US National Security Agency (NSA) accessing Call Data Records (CDRs) from major Pakistani telecom companies to reports indicating that the United Kingdom Government Communications Headquarters (UK GCHQ) had hacked into the routers that controlled the flow of Internet traffic in order to acquire sensitive data.[127]

At the international level, Pakistan is a member of Asia Pacific Computer Emergency Response Team (APCERT) as well as Organisation of the Islamic Cooperation–Computer Emergency Response Team (OIC-CERT). Pakistan was also a member of the UN GGE set up in 2013 to consider developments in the field of information and telecommunications in the context of international security. The sudden importance of Pakistan was reflected in the joint statement following the visit of Pakistan Prime Minister, Nawaz Sharif to the United States in October 2015 that contained a paragraph on cybersecurity. It read: "Recognizing the opportunities and challenges presented by information and communications technologies, President Obama and Prime Minister Sharif affirmed that international cooperation is essential to make cyberspace secure and stable. Both leaders endorsed the consensus report of the 2015 UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security. The leaders looked forward to further multilateral engagement, and discussion of cyber issues as part of the US-Pakistan Strategic Dialogue."[128]

---

[127] "UK Hacked Routers to Monitor Pakistan Communications Data: Snowden", *The Express Tribune*, 6 October 2015, available at http://tribune.com.pk/story/968194/uk-hacked-routers-to-monitor-pakistan-communications-data-snowden/, accessed on 26 November 2015.

[128] "2015 Joint Statement by President Barack Obama and Prime Minister Nawaz Sharif", The White House, 22 October 2015, available at https://www.whitehouse.gov/the-press-office/2015/10/22/2015-joint-statement-president-barack-obama-and-prime-minister-nawaz, accessed on 27 November 2015.

The nodal authority for investigating cybercrime is the National Response Centre for Cyber Crime (NR3C) which was created in 2007 as a body of the Federal Investigative Agency. This body has become Pakistan's *de facto* CERT. [129]

Pakistan does not yet have a national cybersecurity policy though a draft policy was brought out in 2021.[130] Nor does it have a CERT at the time of writing. A National Centre for Cyber Security was established at the Air University in 2018 with the aim of dealing with cybersecurity challenges in the digital age. Locating the centre in a university would indicate that the major focus would be on research and development, which is further borne out by news reports. [131]

Bangladesh

According to the Bangladesh Telecom Regulatory Commission, the total number of Internet subscribers in Bangladesh amounted to 44 million (28 per cent of the population) of which 96 per cent accessed the Internet through mobile telephony. Only 0.8 per cent had access through wired broadband. International connectivity was through a lone Southeast Asia–Middle East–Western Europe (SEA–ME–WE) 4 submarine cable system till 2017 when a second cable was connected to SEA–ME–WE 5.[132] Even with the completion of this cable, about

---

[129] See http://www.fia.gov.pk/en/NR3C.php, accessed on 17 June 2013.

[130] Tahir Amin, "Ministry Drafts National Cyber Security Policy 2021", *Brecorder*, 29 January 2021, available at www.brecorder.com/news/40057558, accessed on 15 February 2021.

[131] According to these reports, the Air University has also developed the curriculum for a four-year BS Cyber Security program. Afshan S. Khan, "'NCCS to Develop Tools to Protect Pakistan's Cyber Space'", *The News International*, 21 May 2018, available at www.thenews.com.pk/print/319672-nccs-to-develop-tools-to-protect-pakistan-s-cyber-space, accessed on 18 April 2019.

[132] "New Submarine Cable Goes Live Sunday", *The Daily Star*, 7 September 2017, available at www.thedailystar.net/business/new-submarine-cable-goes-live-sunday-1459042, accessed on 14 June 2018.

30 per cent of Bangladesh's total bandwidth usage of 565 GBPs came from India. Plans for a third cable have been initiated.[133]

As far as institutional bodies are concerned the relevant bodies are the Bangladesh Computer Council (BCC) and the Bangladesh Telecommunication Regulatory Commission (BTRC). While the BCC was established by an Act of Parliament in 1990, the BTRC was established in 2001.

As far as legislation is concerned, an IT Act was passed by Parliament in 2006. The Act enumerated different cybercrimes and provided for a special court, a Cyber Tribunal, to ensure speedy trial of offences under the Act. Other authorities established under the Act included a Controller of Certifying Authority to facilitate e-commerce. A number of guidelines have also been issued over the years including the Information Security Guidelines 2014 and the National Cyber Security Strategy of Bangladesh 2014.[134] The official Computer Incident Response Team (CIRT), established in 2015 has the limited constituency of all governmental institutions of Bangladesh. Within that constituency, it has a mandate to support government efforts to develop and amplify ICT programmes by establishing incident management capabilities within Bangladesh, which will make these programmes more efficient and reliable.[135] It has a total of nine people working in five teams. An unofficial CERT formed by the local Internet Service Providers (ISPs),

---

[133] Muhammad Zahidul Islam, "Govt Works on 3rd Submarine Cable", *The Daily Star*, 13 March 2018, available at www.thedailystar.net/business/telecom/govt-works-3rd-submarine-cable-1547977, accessed on 17 June 2018.

[134] Gazi Mizanur Rahman, "CYBER CRIMES: A Threat That Must Be Countered", *The Daily Star*, 18 June 2015, available at http://www.thedailystar.net/op-ed/cyber-crimes-threat-must-be-countered-99202, accessed on 26 November 2015.

[135] Bangladesh e-Government Computer Incident Response Team, "About Us | BGD e-GOV CIRT | Bangladesh e-Government Computer Incident Response Team", *BGD EGOV CIRT Bangladesh EGovernment Computer Incident Response Team*, available at www.cirt.gov.bd/about-us/

Bangladesh Computer Emergency Response Team (bdCERT), was in existence for about 10 years before the establishment of the official CERT.[136]

Provisions of the Act were used to ban Facebook in May 2010, leading to a challenge in the law courts on the legality of such a ban. The Act was amended in 2013 but was widely criticised for being too draconian. Like in other countries in the region, the focus of the authorities is on maintaining law and order through the control and regulation of social media.

Subsequently, there was a renewed focus on cybersecurity, with first the promulgation of the National Cybersecurity Strategy which set out the goal of "Working collaboratively home and abroad, to manage all major cyber risks that affect us directly irrespective of their origin and type, thereby creating a safe, secure and resilient critical national information infrastructure for our economy and society." The Strategy aligned itself closely with the Global Cybersecurity Agenda of the International Telecommunication Union (ITU) and laid out a number of priorities including improving legal capabilities, technical and procedural capabilities and organisational structures. The aim was to create a coherent vision for 2021 keeping Bangladesh secure and prosperous by coordinating government, private sector, citizens and international cyberspace defence efforts.

In pursuance of this goal, a National Cybersecurity Act was drafted in 2015. The preamble of the Act stated that it was "an act to provide measures for national cybersecurity and for the prevention, detection, response and prosecution of cybercrimes and other related matters." The draft suggested a minimum five years of jail for those who erase or distort someone else's data or send electronic messages with false information to deceive a person. Taking photographs of others secretly and publishing them without permission would be considered a cybercrime with a provision for imprisonment of up to 10 years. It

---

[136] "About Us", BdCERT, available at http://www.bdcert.org/about_bdcert.html, accessed on 18 July 2018.

also had provision for the security of critical infrastructure which it defined as "assets, system and networks, whether physical or virtual, so vital to the security, defence or international relations of Bangladesh; the provisions of service directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure or the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services."[137]

According to critics, the Act was less to do with cybersecurity and more to do with controlling social media. Among the provisions in the draft Act was one for maximum 20 years of imprisonment for committing "cyber terrorism", and arrest of suspects without any warrant. According to the draft, a crime committed online with its effect in another country would be considered cyber terrorism.[138] In the event, a modified version of the Bill was passed in parliament, culminating in the promulgation of the Digital Security Act in 2018.[139] As with the previous drafts, this law has also been criticised for having excess focus on issues like defamation and controlling social networks rather than cyber and digital security, the title notwithstanding.[140]

---

[137] Much of the text seems to be taken out of the Nigerian Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 since Nigeria is inadvertently mentioned in the draft text on p.15, available at http://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/notices/9c13a044_fafc_4c8e_9e8b_92589ea683a2/Cyber%20Security%20Act%20Bangla%20(10.03.15)%20(1).doc, accessed on 14 July 2018.

[138] "Review Body Formed to Check Draft", *The Daily Star,* 5 July 2015, available at http://www.thedailystar.net/frontpage/review-body-formed-check-draft-108010, accessed on 26 November 2015.

[139] "Digital Security Act Formulated to Control Cyber Crimes", *Dhaka Tribune*, 21 October 2018, available at www.dhakatribune.com/bangladesh/law-rights/2018/10/21/inu-digital-security-act-formulated-to-control-cyber-crimes, accessed on 17 November 2018.

[140] Faisal Mahmud, "Bangladesh Enacts New Law That Could Silence Dissenters", *The Diplomat*, 10 October 2018, available at thediplomat.com/2018/10/bangladesh-enacts-new-law-that-could-silence-dissenters/, accessed on 12 November 2018.

It would seem that the focus of Bangladeshi authorities is primarily on social networks which have "been used to execute criminal acts and incite communal riots". This notwithstanding, Bangladesh was the target of one of the most audacious attempts at cybercrime in 2016, with the Central Bank of Bangladesh almost losing over a billion dollars to cyber-criminals who attempted to manipulate the SWIFT system.[141] As with most such incidents, the chain of events traversed the globe from Sri Lanka to the Philippines, and the criminals are yet to be caught with much speculation that insiders who knew the vulnerabilities of the system were involved.

Sri Lanka

Sri Lanka has about 5 million Internet users in a country of 19 million, making up about 21 per cent of the population. Being an island state, it depends on a combination of submarine cables and satellites for Internet connectivity. There are as many as seven submarine cables servicing Sri Lanka.

As in other countries in the region, the early impetus for legislation was provided by the outsourcing boom and the need for appropriate legislation to cover data protection. The legal and technical frameworks have developed organically over the years. Paramount in the development of the legal framework was the establishment of a Computer and Information Technology Council (CINTEC) Law Committee in 1984. Successive acts developed and passed under the auspices of the CINTEC were the Evidence (Special Provisions) Act No.14 of 1995 (include computer related evidence to the Evidence Ordinance of 1895), the Electronic Transactions Act of 2006 and the Computer Crimes Act of 2007.

The Act covered two categories of offences, which are: (1) when a computer was used in the commission of a crime such as theft and fraud; and (2) crimes carried out through the Internet such as hacking.

---

[141] "The Billion-Dollar Bank Job", *The New York Times*, 3 May 2018, available at www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html, accessed on 17 November 2018.

The Act also provides for an independent group of experts to assist law enforcement agencies in the investigation of Cyber Crime, making them almost on par with police officers.[142] A subsequent section also sought to safeguard businesses from undue suffering as a result of investigation into a crime.[143]

Criticism of the Act has been mainly about Section 18(2) which allows investigating agencies to carry out warrantless wiretapping if deemed urgent. Privacy advocates have said that this privileges law enforcement over privacy while others feel that the use of this provision is the exception rather than the rule. In 2015, Sri Lanka became the only second Asian country after Japan to accede to the Budapest Convention on Cybercrime.

On the policy side, the Information and Communication Technology Agency (ICTA) of Sri Lanka is the apex ICT institution of the government. In terms of the Information and Communication Technology Act No. 27 of 2003 (ICT Act), ICTA has been mandated to take all necessary measures to implement the Government's Policy and Action Plan in relation to ICT.

On the technical side, the Sri Lanka Computer Emergency Response Team (SLCERT) was created in 2006 to address cyber security incidents. This is a government-owned company (a subsidiary of ICT Agency of Sri Lanka–ICTA), established with support from World Bank, and runs on a private sector driven model with highly skilled incident handlers. The Board consists of a range of key stakeholders such as enforcement authorities, bankers, private sector and academia. The SLCERT was admitted as a member of APCERT and became the first South Asian CERT to be admitted as a member of Forum of Incident Response and Security Teams (FIRST) in 2008. Due to the requests from law enforcement agencies, SLCERT started offering digital forensics as a service for law enforcement agencies since the

---

142 Section 17 of the Computer Crimes Act No. 24 of 2007.

143 Section 20 of the Computer Crimes Act No. 24 of 2007.

third quarter of 2008. The SLCERT also carries out forensic investigations for other government establishments in Sri Lanka.[144] Sri Lanka participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).[145] Since 2008, an annual Cyber Security Week (CSW) programme which consists of a national cyber security conference, workshops, seminars, media campaigns, hacking challenges for students, etc., has been held every year by SLCERT.

Internet is accessed by well over 10 million people which amounts to Internet penetration of 38 per cent in a population of 31 million. About 95 per cent of this is through Mobile Internet Services.[146]

The main cyber related laws are mentioned in the Electronic Transactions Act 2004, which defines and sets penalties for computer and cybercrimes, such as hacking, piracy and computer fraud. Complaints have to be made within 35 days of awareness of the crime.

A National Information and Cyber Security Strategy was approved by the Council of Ministers in October 2018. It was developed in consultation with the European Union, with the implementing partners being the United Kingdom, the Netherlands and Estonia. A Cyber Security Act has also been proposed.[147]

---

144 Jayanto Fernando, "Cybercrime Legislation - Sri Lankan Update", available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f264b, accessed on 7 January 2019.

145 "Drill to Tighten Global Network in Fight against Cyber Attacks," International Telecommunication Union, 20 May 2014, available at http://www.itu.int/net/pressoffice/press_releases/2014/26.aspx#.Vl_qJ1grLcs, accessed on 3 December 2015.

146 "Internet Access Reaches to One-third Population in Nepal", *Kathmandu Today*, 20 February 2015, available at http://www.ktm2day.com/2015/02/20/internet-access-reaches-to-one-third-population-in-nepal/, accessed on 4 December 2015.

147 Indunil Hewage, "Govt to Enact Cyber Security Act within next Two Months", *Daily News*, 22 March 2019, available at www.dailynews.lk/2019/03/22/business/180962/govt-enact-cyber-security-act-within-next-two-months, accessed on 22 June 2019.

Bhutan

Bhutan had 7,79,966 Internet users amounting to 95 per cent of the population in 2014. Out of these, 22,000 were fixed broadband subscribers while 7,03,000 were mobile subscribers.[148] Bhutan has two international gateways, one at Phuentsholing and the other at Gelephu, both of which connect to Siliguri.[149] A third Internet gateway has been planned via Bangladesh.[150]

The Information Communications & Media ACT of 2006 was a comprehensive act providing, as mentioned in the Preamble "for a modern technology-neutral and service sector-neutral regulatory mechanism which implements convergence of information, computing, media, communications technologies and facilitates for the provision of a whole range of new services". It was subsequently repealed with the promulgation of the Bhutan Information and Communications and Media Act (BICM Act) 2018. [151] Like the earlier act, this too covered the gamut of ICT and media services with Chapter 20 being devoted to cybersecurity. It provided for the establishment of Bhutan Computer Incident Response Team (BtCIRT) national agency to coordinate cybersecurity activities and be a central point of contact on all cybersecurity matters pertinent to national security in the country.[152]

---

148 Bhutan, Ministry of Information Technology and Communications, Annual Info-Comm and Transport Statistical Bulletin, 10th Edition, 11 February 2019, available at https://www.moic.gov.bt/wp-content/uploads/2019/03/10th-Annual-Info-Comm-and-Transport-Statistical-Bulletin-2019.pdf, accessed on 18 June 2019.

149 "The New Internet Gateway", *Thimphu Today*, 26 March 2012, available at http://www.thimphutech.com/2012/03/new-internet-gateway.html, accessed on 6 December 2015.

150 "Third International Internet Gateway Prioritised in 12th Plan", *KuenselOnline*, 28 April 2018, at www.kuenselonline.com/third-international-internet-gateway-priortised-in-12th-plan/, accessed on 17 May 2018.

151 Bhutan Infocomm and Media Authority, available at http://www.bicma.gov.bt/bicmanew/data/publications/act/BICM_Act_2018_English.pdf, accessed on 18 January 2019.

152 Ibid., p. 119.

The Act also equated offline rights of citizens with online rights, declaring that all forms of personal rights and security accorded to the citizens shall be protected in the cyberworld.[153] The responsibility for its enforcement is vested with the Bhutan Info-Comm & Media Authority (BICMA). Other policies include the Bhutan Information Management and Security Policy 2009 and a draft of the Bhutan Cybersecurity Strategy 2018.

A national CERT was set up with financial assistance from the World Bank and became operational in 2016.[154]

Afghanistan

As per the International Telecommunication Union (ITU) statistics, there are nearly 4 million Internet subscribers in Afghanistan, an Internet penetration of 11 per cent. According to Afghanistan's Ministry of Information Technology, in 2014, mobile subscribers added up to 7,50,000 while wired broadband subscribers are only about 20,000.[155] More recent unofficial estimates put the number of people accessing the Internet on mobiles at 3.2 million. Much of Afghanistan's telecommunication was destroyed or damaged during the Afghan conflict, and though a lot of the infrastructure has been rebuilt, it is still subject to disruption from ongoing conflict.

An Afghanistan Cyber Emergency Response Team (AFCERT) was established in 2009. The mandate of AFCERT was to fight against cyber threats and crimes. The AFCERT also undertook an exercise to

---

153 Ibid., p. 118.

154 "Cyber Security Team to Be Formed by Next Year", *KuenselOnline*, 28 August 2015, available at http://www.kuenselonline.com/cyber-security-team-to-be-formed-by-next-year/, accessed on 6 December 2015.

155 An In-Depth Study on the Broadband Infrastructure in Afghanistan and Mongolia April 2015, Rep. United Nations Economic and Social Commission for Asia and the Pacific, Apr. 2015, Web. 7 Dec. 2015, p. 21, available at http://www.unescap.org/sites/default/files/Broadband%20Infrastructure%20in%20Afghanistan%20and%20Mongolia%20v3.pdf, accessed on 3 June 2018.

create a draft National Cyber Security Strategy to coordinate all cyber and information security related issues in the country with clearly defined roles and responsibilities. The draft was released in November 2014.[156] A cybercrime bill was enacted into law in 2017 which "criminalised a range of online activities including hacking, spreading ethnic hatred, distribution of online defamatory speech, exposing government secrets, and cyber-terrorism."[157]

India

India was one of the earliest countries in Asia to set up a CERT. The Computer Emergency Response Team-India (CERT-In) began operations in 2004 with a mandate to "create a safe and secure cyber environment through appropriate policies and legal frameworks". Specific tasks included creating appropriate cybersecurity standards/guidelines, auditing, networking and developing Points of Contact (POCs), conducting cybersecurity drills, devising and deploying crisis management plans and cyber alert systems and interfacing with sectoral and foreign CERTs. The Information Technology Act of 2000, which was primarily concerned with outsourcing, was amended in 2008 with the Information Technology Amendment Act, 2008, which provided for a national nodal agency for critical information infrastructure protection. This agency has been set up after it was decided to make National Technical Research Organisation (NTRO) the nodal agency for critical infrastructure.[158] The National Critical Information Infrastructure Protection Centre (NCIIPC) was established under the

---

[156] Afghanistan. Ministry of Communications and Information Technology, *National Cybersecurity Strategy of Afghanistan* (NCSA), November 2014, available at http://mcit.gov.af/Content/files/National%20Cybersecurity%20Strategy%20of%20Afghanistan%20(November2014).pdf, accessed on 7 December 2015.

[157] "Afghanistan Enacts Law to Control Cyberspace", *The New Indian Express*, 10 July 2017, available at www.newindianexpress.com/world/2017/jul/10/afghanistan-enacts-law-to-control-cyberspace-1626798.html, accessed on 10 August 2017.

[158] "Five-Year Plan in the Works to Revamp Cyber Security", *The Times of India*, 18 December 2012.

NTRO in 2013 as also the office of the National Cyber Security Co-ordinator. A National Cyber Security Policy was also promulgated in 2013 with a new iteration currently before the Union cabinet.

The government has an initiative in place called Digital India with a proposed outlay of over 1,13,000 crores (USD 16 billion). Digital India is conceptualised as a service to the people "where government services are easily and efficiently available on mobile devices; where government actively engages with people on social media; where mobile phones enable personal services; and where cyber security becomes an integral part of the national security". The "Digital India" programme seeks to expand the Internet user base to 600 million and to increase broadband speed to 2Mbps from the present 512 kbps. This is not an end in itself. The programme has nine so-called pillars, which broadly seek to provide digital infrastructure as a utility for every citizen, governance and services on demand and digital empowerment. There are other programmes related to financial inclusion that are closely tied in with this programme. For instance, the issue of debit cards has gone up by 100 million as part of the programme to create bank accounts in rural areas.

This capacity building for citizens also has enormous implications for security, specifically cybersecurity. As more and more people get exposed to technology when they avail government services online, conduct financial transactions through mobiles, or simply surf the Internet using Wi-Fi at colleges, the risks will also go up manifold.

Among the initiatives intended to build capacity in cybersecurity are a National Cyber Security Coordination Centre, an e-Governance Security Centre, initiatives to encourage manufacturing of electronic products within the country and a Centre of Excellence in the "Internet of Things".

As far as the internal challenges are concerned, these would comprise building up capacities to provide a safe and secure cyberspace, improving capabilities in law enforcement, judicial and forensic areas, updating national policies to deal with new challenges from areas like cloud computing and the Internet of Things without hobbling the development of such technologies, improving coordination between various ministries of the government, creating a better interface between

the public sector and the private sector and creating opportunities for manufacturing within the country. These challenges are not unique to India and other countries in the Asia–Pacific region would also be facing similar issues.

As far as the external challenges are concerned, these are equally daunting, requiring complex negotiations on operationalising co-operative relationships (bilateral as well as multi-lateral) while giving greater emphasis to regional cooperation, establishing mechanisms for exchanging information, imbibing best practices through joint exercises and working with others towards viable solutions in the critical areas of supply chain integrity, security standards, internet governance, and law enforcement co-operation.

Given the contestations in the arena of cybersecurity in the realm of international policy making and the enduring insecurities in cyberspace, the countries of South Asia could be said to be easy pickings for the major powers since they are in need of help in building up their cyber capabilities and capacities. The lack, thereof, especially for the smaller countries, render them at the mercy of the major cyber powers to cover their security needs, with the *quid pro quo* being support for their positions in multilateral fora. The absence of regional organisations dealing with cybersecurity means that the interests of this region will not be heard and will be subsumed by other considerations. With military concepts such as *defend forward* coming to the fore as seen in previous chapters, these countries could also become staging grounds for cyber forces.

Chapter 6

Conclusion

Major powers are utilising a variety of strategies, based on their cyber competencies, to leverage their cyber power to coerce and compel both their friends and adversaries to hew to a predetermined path. On a broader strategic level, the mechanisms used are timeworn, as seen in the preceding chapters, including building up military power through the establishment of cyber commands, denial of technology and creating formal and semi-formal alliance mechanisms. In order to be effective, these instruments of cyber power have to be built up, and this has proven to be a difficult and time-consuming exercise requiring political will, administrative finesse and adaptability and clear vision of the strategic goals to be achieved. It requires investment in infrastructure and capabilities with a high probability that these investments might go to waste since cyber technology develops at a very fast pace and has a propensity to branch off in new directions defying even the best-laid plans.

For militaries, it has not only meant adapting existing doctrines, capabilities to cyberspace, but also almost going back to the drawing board and restructuring the military itself, bringing in new institutional capacities and going beyond jointness to integrating with civilian agencies and starting new initiatives to coordinate with the private sector. This has had to be done through negotiating with executive fiat not succeeding beyond a certain point. The difficulties are brought out in the case studies on the United States and France. Other countries continue to struggle in deciding the size and scope of their cyber forces, and in deciding where exactly to locate the nucleus of these capabilities. What the study shows is that creating a cyber force without a doctrine and clear lines of authority is a recipe for confusion. The multipurpose nature of cyber capabilities, ranging from destruction to disruption to espionage, and the potential for misuse of these capabilities, requires verifiable oversight mechanisms.

The purpose of the doctrines is not only to lay out the structure, responsibilities and authorities so that all relevant parties are aware of their roles and responsibilities, but also to lay out the redlines to adversaries to act as a deterrent against any adventure. The doctrine and creation of capabilities have to go hand-in-hand for it to have any effect. On the legal and ethical side, much remains to be discussed, including outcomes such as the collateral damage incurred by third parties and innocent bystanders as a result of cyber-attacks as well as unintended consequences such as the leakage of cyberweapons, most recently seen in the large-scale leakage of the US NSA's inventory of cyber weapons.

A second strategy has been the denial of technology; one that is all the more important in a domain where technology, more than any other factor is the key determinant of dominance. However, as the study of the attempts to adapt the Wassenaar Arrangement to cyberspace shows, even when there is a common goal amongst various states, the complicated and interdependent nature of cyberspace makes it very difficult to implement a denial of technology regime. Multiple influential actors, from academia to private sector companies, working across countries were successfully able to stymie the provisions that would have regressed research and development as well as impacted the profits of these companies. Denial of technology and of natural resources has been used as a strategy more effectively at a country level, with recent instances of the former being the United States putting the Chinese telecommunications giant Huawei on the entity list, thereby cutting its access to US technology. In retaliation, China has threatened to cut off US access to rare earths required for production of hardware, a threat it had carried out successfully against Japan in 2017. A secondary related approach is the denial of market access to adversary countries as most recently seen in US attempts to deny Huawei market access to its 5G products, along with attempts to get US allies to do the same. Though there are few other powers at the moment that have the wherewithal to undertake similar denial of technology actions, most powers would take note of such actions undertaken and would intensify efforts to maintain their national interests and strategic autonomy by diversifying their sources of technology as well as indigenising technology.

Regional and sub-regional groupings have been accorded an important role in implementing recommendations of UN bodies, and have, therefore, become an important arena in and through which major and middle powers strive to shape the international environment. As seen in the previous chapters, the major powers have gone to the extent of co-opting the middle and minor powers into various fora, and in some cases, virtually hijacking the fora. These fora are therefore an important tool in the quest for cyber power. That notwithstanding, South Asia is the only region that is lacking a sub-regional organisation and therefore misses out on contributing its perspective to the global conversation on cyberspace. As the appraisals of the various countries in the region show, they all have different priorities and are at various stages of maturity. Whatever be the issue, South Asian cooperation has become more of an ad hoc than systemic cooperation because of the constantly shifting relations between the various countries of the region.

In India, the focus has been on improving resilience and cyber defences, and benchmarking the country's cyber capabilities against indexes like the annual Global Cybersecurity Index brought out by ITU. In the last such assessment brought out in 2018, India ranked 23 with the Indian National Cybersecurity Co-ordinator setting a goal for India to enter the top 10.[159] The country that ranked first, Singapore, also achieved the goal after Gulshan Rai's counterpart in the Cyber Security Agency of Singapore put out a similar challenge to his team.

Whilst a Cyber Command is taking shape slowly, with the establishment of a Cyber Defence Agency, there is an urgent need to publish a doctrine to put in place its roles and responsibilities, and more importantly, to delineate them *vis-à-vis* other agencies. As the US case study shows, much of the hard work begins only after the policy decisions are made, since existing capabilities have to be integrated not only within the military but also across other government agencies and the private sector. India has recognised the need for a regional forum and is pushing BIMSTEC initiatives in cybersecurity but much more has to be brought to the

[159] This goal was achieved in 2021 when India was ranked No. 10 in the list.

table, including funding and expertise. For this, research and development on cyber technologies should be reinvigorated to not just enable India to take its rightful place as a leading cyber power, but also to ensure that it is not affected by technology denial regimes, which have a tendency to cause collateral damage.

Appendix 1

France - Unclassified Elements of The Military Doctrine on Offensive Cyber Operations[160]

In a geopolitical environment plagued by crises, destabilization, terrorist threats, and conventional and hybrid wars, the Ministry of the Armies helps to guarantee, in all circumstances, in times of peace or war, the national sovereignty and autonomy of decision making of France, on its territory as was as in all theaters where our armies happen to be deployed.

The cyberattacks against Estonia= in 2007, against the electricity networks of Ukraine, against TV5 Monde in 2015, the ransomware Wannacry in the spring of 2017 or the NotPetya attack in June 2017, illustrate the possible fields for attackers whose four major objectives are espionage, illicit trafficking, destabilization and sabotage.

Most power struggles, crises and contemporary conflicts are developing in the digital space. Armies must now systematically, look at cybernetic combat as a mode of action in its own right whose effects combine with others in a global manoeuvre.

A true break in terms of technology and the use of force, the cyber weapon is destined to upset the modalities of the war without profoundly reshaping its principles. Multiplicity of state actors,

---

[160] France, Ministry of Defence, P*ublics de Doctrine Militaire de Lutte Informatique Offensive,* available at https://www.defense.gouv.fr/content/download/551555/9394645/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf, accessed on 15 November 2019. Unofficial translation.

anonymous or otherwise, terrorist organizations, blurred borders, awareness limitations, distorted points of reference, rapid propagation, international law not respected, code of conduct flouted: these are the risks of cyberspace. A grey area, a fog, whose effects are real, sometimes devastating. The fight in cyberspace is asymmetrical, hybrid, sometimes invisible and seemingly painless. Yet the use of the cyber weapon is likely to seriously undermine the capabilities and sovereign interests of States.

The Cyber Defence Strategic Review, published in February 2018, confirmed the relevance of our organizational and governance model that separates missions and offensive capabilities from defensive missions and capabilities. It has proposed a full-fledged strategy in this area by structuring the organization of cyber defence around an inter-ministerial coordination centre of cyber crises led by the General Secretariat for Defense and National Security (SGDSN) under the authority of the Prime Minister and four separate operational chains. In addition to the "protection", "intelligence" and "forensic investigation" chains, the "military action" chain has notably resorted to offensive cyber warfare (LIO).

France is thus consolidating a renewed model of cyber defence, including the creation of the Cyber Defence Command (COMCYBER) in May 2017 has been one of foundational steps by the Ministry of the Armed Forces.[161] The COMCYBER is responsible for military cyber defence, which encompasses all cyber defensive and offensive actions conducted in cyberspace to ensure the effective functioning of the Ministry and the effectiveness of the armed forces, in the preparation, planning and conduct of military operations.

Going forward, the Ministry of the Armed Forces has capacities and a doctrine which covers cyber offensive actions dedicated to the engagement of the armed forces.

---

[161] Decree n ° 2017-743 of May 4th, 2017 relating to the attributions of the chief of staff of the armies and the decree of May 4th, 2017 modifying the organization of the staff of the armies.

ACT IN CYBERSPACE: offensive cyber operations for military purposes, a weapon of operational superiority

The ability to conduct defensive and offensive military operations in cyberspace helps to ensure national sovereignty. It contributes not only in the obtaining of operational advantages in the theatres of engagement of our armed forces, but also in the defence of the information systems of the armies. Thus, the armed forces equip themselves with the whole spectrum of the means of computer control now necessary for the conduct of the operations: defensive, offensive and against the manipulations of the information harmful to our military operations.

Under the authority of the Chief of the Défense Staff, the COMCYBER is the authority in charge of cyber offensive military capability deployment, an integral part of the operational chain of operations with a fully consistent organization and operational structure.

1) OFFENSIVE CYBER OPERATION FOR MILITARY PURPOSES: DEVELOPING A FLEXIBLE AND INNOVATIVE CAPACITY

The offensive cyber operations for military purposes (LIO) covers all actions undertaken in cyberspace, conducted autonomously or in combination with conventional military means. The cyber weapon aims, in strict compliance with international rules,[162] to produce effects against an adversary system to alter the availability or confidentiality of the data.

The variety of the effects of offensive cyber operations and the corresponding modes of action are due to the nature of cyberspace, which is a new field of confrontation. It is based on a three-layer structure:

- a physical layer made up of the equipment of computer systems and their networks having a material existence and, for some of

---

[162] As stated in the strategic cyber defense review, these rules define the conditions leading to the triggering or retaliatory measures, countermeasures or even the use of force in case of armed aggression justifying self-defense.

them, an electromagnetic existence (computers, processors, cables, fibres, transmitters, receivers, satellite links, routers, etc.).

- a logical layer, made up of all the digital data, the processes and tools for managing and administering this data, as well as their exchange flows (files, sites, addresses, connection codes, protocols, software applications, etc.), implemented in the hardware to enable them to deliver the services expected.

- a semantic and social layer, consisting of information circulating in cyberspace and by people who may have multiple digital identities or "avatars" (pseudonyms, e-mail addresses, IP addresses, blogs, etc.

The interdependence of these three layers offers opportunities for offensive cyber operations with the goal of destabilizing the opponent.

When combined with conventional modes of action, offensive cyber operations can amplify, enhance or complement these actions and have a multiplier effect since cyber networks are part of the growing networking of all military systems and deeply interconnected through the Internet.

The use of offensive information operations is part of a temporality of its own. Although its effects can be dazzling, its integration into the overall operational manoeuvre is a process characterized by long and very specific planning. These effects can be of a material nature neutralization of a weapon system, or intangible—intelligence gathering, temporary, reversible or definitive.

2) OBJECTIVE OF OFFENSIVE INFORMATION OPERATIONS: TO CONTRIBUTE TO MILITARY SUPERIORITY IN CYBERSPACE

In the face of an adversary, offensive information operations offer discrete and effective modes of action against digitized systems, capable of substituting for other modes of action, of preparing for them or contributing to their successful completion.

Offensive information operations makes it possible to take advantage of vulnerabilities in opposing digital systems during all phases of a crisis: intelligence, prevention, management or stabilisation.

It achieves three types of operational objectives in the conduct of military operations: (1) evaluation of enemy military capabilities: collection or extraction of information, (2) reduction or even neutralization of enemy capabilities: temporary disruption or creation of major damage in the enemy's military capabilities and (3) modification of the adversary's perceptions or analytical capacity: discrete alteration of data or systems, exploitation of stolen information obtained from within an adversary's military information system.

Targets may be exposed on the Internet, isolated, or part of a larger weapons system. The offensive information operations contribute to securing and even preserving the digitized resources used by our deployed forces. Offensive information operations are not necessarily conducted through physical contact of the opponent.

Offensive information operations can also be in support of a cyber defence manoeuvre when a cyber-attack exclusively targets the operational capabilities of the armed forces or the defence chains of command by its use in the characterization of an attack, by putting an end to a cyber aggression on our systems, in accordance with the article L. 2321-2 of the defence code[163] or by imposing a diversion of the attacker's efforts towards useless targets.

Complementing conventional weapons, the IOL produces the same effects of intelligence, neutralization or deception in a new domain.

It may be used in substitution or in combination with other capacities of collection or action on the whole spectrum of the military engagement: to inform, to defend, to act.

---

[163] Article 21 of Law No. 2013–1168 of 18 December 2013 on military programming for the years 2014–2019 contain the various provisions concerning defense and national security.

OPERATIONAL FUNCTIONS OF OFFENSIVE INFORMATION OPERATIONS

Analysis	DEFEND	ACT
Characterise and assign opposing systems	Identification of the attacker	Counter misinformation
Watch the opponent	Retaliation: digital intervention in the event of intrusion Neutralization in accordance with Art. L. 2321-2 of the Défense Code	Aiding the conventional military manoeuvre by disrupting or neutralizing the enemy's military capabilities

ORGANIZATION OF THE OFFENSIVE INFORMATION OPERATIONS: A UNIFIED CHAIN OF COMMAND, SPECIALIZED UNITS

Offensive information operations rely on sensitive know-how and is one of the attributes of a sovereign defence. These two dimensions require strategic control of offensive information operations, from planning to implementation.

Under the authority of the President of the Republic and under the orders of the Chief of Defence Staff, the COMCYBER is responsible for planning and coordinating offensive information operations for joint operations. He ensures the coherence of the planning and conduct of offensive information operations with the various other operational staffs (joint, ground, naval, air, special forces), and the intelligence services, from the strategic level to the tactical level. Finally, he develops and animates the LIO component of military cooperation with the allies.

Offensive information operations works at the strategic level (in global joint operations) and tactical (in joint operations by the various arms of the Forces).

EXAMPLES OF OFFENSIVE INFORMATION OPERATIONS USE AT TACTICAL LEVEL AND STRATEGIC LEVEL

	Tactical level jobs	Strategic level jobs
Evaluation of opposing forces	- Intelligence of immediate interest related to the action of the forces	- Intelligence in preparation of the operations, for purposes of targeting or capacity development
Reduction or even neutralization of opposing forces	- Neutralization of a weapon system - Neutralization of a command post	- Neutralization of an enemy's operational capability (example: propaganda vector), - Neutralization of a strategic level command system
Action on perceptions or the ability to analyse adversely	- Alteration of the data of a command system	- Sowing confusion in enemy propaganda centres

Offensive cyber operations are conducted by specialized units, whose expertise guarantees adequate risk analysis of and control of the effects, collateral or even fratricidal, a result by the complexity of the operational area. The action of these specialized units is fully integrated into the armies manoeuvring, directly on the ground or at a distance.

CONTROLLING RISKS RELATED TO THE USE OF THE IOL: a *sine qua non* of any operation

Under the command of General Officer COMCYBER, the use of the offensive information operations requires an absolute control of political, judicial, and military risks at all stages of the operation.

Like any military operation, offensive information operations implies an acceptance of risk at the decision-making level, determined by the

principles of *jus in bello* (proportionality, distinction, discrimination, ...), the cost-effectiveness ratio, the operational situation and the general political context.

The risks associated with the use of the offensive information operations come primarily from the characteristics of cyberspace: rapidity of action, duality of targets and hyper connectivity.

In addition, the sophisticated means and modes of action designed to carry out these actions require strict control and control of their end-to-end use, in particular in order to avoid any risk of diversion, compromise or collateral damage. Indeed, offensive information operations can have effects beyond the intended target because of the unknowns of configuration and interdependencies between systems, increasingly common in cyberspace. In addition, an information operations tool can be stolen, copied or imitated by opponents or third parties. It does not generally include the constraints associated with threshold weapons reserved for States with a certain technological maturity.

Finally, opponents with offensive capabilities, but with a smaller area of digital vulnerability, could be less risky in a conflict escalation against our interests.

In order to maintain its effectiveness and control the risks of diversion, all offensive information operations conducted by the armed forces remain secret in nature, but political and military authorities may, depending on the circumstances, announce them publicly and even claim them. This posture is a matter of political decision. The decision to publicize an offensive information operation must ultimately be weighed against the risk of the vulnerability inherent in the high digitization of our national interests.

LEGALLY JUSTIFYING OFFENSIVE CYBER OPERATIONS: A Necessity and Protection

Offensive information operations are subject, like any other weapon or method of war, to the principles and rules of international law, including international humanitarian law, as well as to national laws and

regulations. It is therefore used only in compliance with very restrictive operational rules of engagement.

When carried out in support of the cyber defence activity, offensive information operations are conducted, under the responsibility of the Chief of Staff of the Armed Forces, within the framework defined in the internal law by the code of defence and under the conditions set by the Prime Minister.

France is seeking the adoption of rules of responsible behaviour and international codes of good conduct to prevent situations of conflict in cyberspace, to guarantee its strategic stability and, if necessary, eventually to serve as a reference for possible developments in international law.

DEVELOPING A SHARED CULTURE OF OFFENSIVE INFORMATION OPERATIONS: EFFECTS TO INTEGRATE IN COALITION

France is a major player in NATO and European partnerships in the cyber sector.

Cooperation in cyberspace is not self-evident and is part of a complex logic. In the face of the cyber threat, disparities in capabilities, organization, doctrines and investments of the partners constitute an additional difficulty. That is why, in 2016, within the framework of NATO, France and its allies signed a commitment inviting member countries to equip themselves with cyber means to ensure their individual and consequently collective security: the Cyber Defence Pledge. In the continuation of this commitment, France is committed, like its main partners, to share the effects produced by its own means of offensive information operations for defence purposes or collective military operations, but always national control because they come under our strict sovereignty.

At the European level, France plays a leading role in promoting a shared cyber military culture and aims to develop operational interoperability with our main European partners.

France's international commitments in the cyber sector, illustrated by the signing of MoU or technical approvals governing cooperation,

testify to the will to build a cyber defence policy with international partners across the spectrum (LID and LIO); a necessity today indispensable to the defence of our strategic interests.

TAKING UP A CHALLENGE FOR THE FUTURE: Offensive Information Operations, An operational Military Capability to be Developed

The development of offensive computer control capabilities for the benefit of armies is entrusted to the Directorate General of Armaments (DGA), as for any other military capability. Due to the sensitivity and dynamics of the field, the COMCYBER teams and the cyber teams of the DGA work in close cooperation in the development and implementation of a capability roadmap.

Offensive information operations must continue to be developed around five main challenges:

- Speed up the production of offensive computer control resources for the benefit of the armed forces.
- Define an HR policy that will make it possible to respond to the expertise challenges of this new capacity.
- Undertake training activities for the use of the IOL for military purposes, within the staffs of planning and conducting joint operations.
- Adapt our capacity acquisition and development processes to the dynamics and speed of innovation in the cyber world.
- Converge with partners, in particular European partners, on operational ambitions to allow us to act in coalition including in a crisis or a war theatre.

Appendix 2

Command Vision for US Cyber Command[164]

Military superiority in the air, land, sea, and space domains is critical to our ability to defend our interests and protect our values. Achieving superiority in the physical domains in no small part depends on superiority in cyberspace. Yet we risk ceding cyberspace superiority. As the 2018 National Defense Strategy explains, adversaries are increasingly capable of contesting and disrupting America's society, economy, and military. This is in part because of our growing reliance on cyberspace. Adversaries direct continuous operations and activities against our allies and us in campaigns short of open warfare to achieve competitive advantage and impair US interests. The cyberspace domain that existed at the creation of US Cyber Command (USCYBERCOM) has changed. Our adversaries have exploited the velocity and volume of data and events in cyberspace to make the domain more hostile. They have raised the stakes for our nation and allies. In order to improve security and stability, we need a new approach.

As the nation's cyber warriors, USCYBERCOM operates daily in cyberspace against capable adversaries, some of whom are now near-peer competitors in this domain. We have learned we must stop attacks before they penetrate our cyber defenses or impair our military forces; and through persistent, integrated operations, we can influence adversary behavior and introduce uncertainty into their calculations. Our forces must be agile, our partnerships operational, and our operations continuous. Policies, doctrine, and processes should keep pace with the speed of events in cyberspace to maintain decisive advantage.

---

[164] US Cyber Command, Mission Document, 2018, available at https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, accessed on 17 September 2019.

Superior strategic effects depend on the alignment of operations, capabilities, and processes, and the seamless integration of intelligence with operations. Now we must apply this experience by scaling to the magnitude of the threat, removing constraints on our speed and agility, and manoeuvring to counter adversaries and enhance our national security.

This document is a roadmap for USCYBERCOM to achieve and maintain superiority in cyberspace as we direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and foreign partners. As a Unified Combatant Command, we will demonstrate our resolve against cyberspace threats. We will unify cyberspace operations. We will secure networks, platforms, and data. We will expand the military options available to national leaders and operational commanders.

This document supports the 2018 National Defense Strategy by posturing USCYBERCOM to counter increasingly aggressive competitors and builds on the Commander's Vision, Beyond the Build: Delivering Outcomes through Cyberspace (June 2015).

Strategic Context

The security of the United States and our allies depends on international stability and global prosperity. The spread of technology and communications has enabled new means of influence and coercion. Adversaries continuously operate against us below the threshold of armed conflict. In this "new normal," our adversaries are extending their influence without resorting to physical aggression. They provoke and intimidate our citizens and enterprises without fear of legal or military consequences. They understand the constraints under which the United States chooses to operate in cyberspace, including our traditionally high threshold for response to adversary activity. They use this insight to exploit our dependencies and vulnerabilities in cyberspace and use our systems, processes, and values against us to weaken our democratic institutions and gain economic, diplomatic, and military advantages.

Cyberspace threats are growing. They transcend geographic boundaries and are usually trans-regional in nature. States possess resources and

patience to sustain sophisticated cyber campaigns to penetrate even well-protected networks, manipulate software and data, and destroy data, computers, and systems. Russia, China, Iran, and North Korea invest in military capabilities that reduce our military's competitive advantages and compromise our national security. Some of these states have demonstrated the resolve, technical capability, and persistence to undertake strategic cyberspace campaigns, including theft of intellectual property and personally identifiable information that are vital to our defenses. Disruptive technologies will eventually accelerate our adversaries' ability to impose costs.

Aggressive non-state actors like terrorists, criminals, and hacktivists pose lesser threats than states but can still damage our military capabilities and critical infrastructure, as well as endanger American lives. Violent extremist organizations, such as the Islamic State of Iraq and Syria, al-Qaida, and affiliated groups, are destabilizing whole regions, attacking our global interests, and endangering our homeland and citizens around the world. These groups use cyberspace to promote their ideology, inspire followers, and control operations that threaten our allies and us. Organized criminal groups provide cover for states and terrorists, and possess significant capabilities to steal data and disrupt government functions. Hacktivists work to expose classified information or impair government services. These malicious cyber actors frequently pose threats that law enforcement and diplomatic means cannot contain without military assistance.

Operating Environment

Cyberspace is a fluid environment of constant contact and shifting terrain. New vulnerabilities and opportunities continually arise as new terrain emerges. No target remains static; no offensive or defensive capability remains indefinitely effective; and no advantage is permanent. Well-defended cyber terrain is attainable but continually at risk. Adversary offensive activities persist because opportunity costs are low, and accesses, platforms, and payloads can remain useful for extended periods.

The underlying technologies and protocols of cyberspace enable both legitimate and malicious activities. Adversaries exploit and weaponize

vulnerabilities to steal wealth and intellectual property, manipulate information, and create malicious software capable of disrupting or destroying systems. The constant innovation of disruptive technologies offers all actors new opportunities for exploitation. In this dynamic environment, the United States must increase resiliency, defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage. We achieve success by seizing the initiative, retaining momentum, and disrupting our adversaries' freedom of action.

National Policy Framework

As the 2018 National Defense Strategy emphasizes, our ability to prevail in strategic competition requires the seamless integration of all instruments of national power. US cyberspace operations can make positive contributions to diplomatic power by providing fast, temporary, and reversible sanctions or communicating discreetly to the adversary. Cyberspace capabilities are key to identifying and disrupting adversaries' information operations. They facilitate overmatch of adversary military capabilities in all domains, expanding options for our decision makers and operational commanders, and producing integrated effects. Insights and threat information gleaned from operating in cyberspace can make key elements of economic power more resilient and defensible.

Whole-of-government approaches for protecting, defending, and operating in cyberspace must keep pace with the dynamics of this domain. We should not wait until an adversary is in our networks or on our systems to act with unified responses across agencies regardless of sector or geography. We cede our freedom of action with lengthy approval processes that delay US responses or set a very high threshold for responding to malicious cyber activities. Our adversaries manoeuvre deep into our networks, forcing the US government into a reactive mode after intrusions and attacks that cost us greatly and provide them high returns. This reactive posture introduces unacceptable risk to our systems, data, decision-making processes, and ultimately our mission success. The Department of Defense (DOD) is building the operational expertise and capacity to meet growing cyberspace threats and stop

cyber aggression before it reaches our networks and systems. We need a policy framework that supports and enables these efforts.

VISION

Achieve and maintain superiority in the cyberspace domain to influence adversary behavior, deliver strategic and operational advantages for the Joint Force, and defend and advance our national interests.

Superiority through Persistence

Superiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver.* It describes how we operate—maneuvering seamlessly between defense and offense across the interconnected battlespace. It describes where we operate—globally, as close as possible to adversaries and their operations. It describes when we operate—continuously, shaping the battlespace. It describes why we operate—to create operational advantage for us while denying the same to our adversaries.

Cyberspace is an active and contested operational space in which superiority is always at risk. We sustain strategic advantage by increasing resiliency, defending forward, and continuously engaging our adversaries. Increased resiliency reduces our attack surface at home, anticipates adversary actions, and increases flexibility in our response. Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and

---

* Cyberspace superiority is the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary (JP 1-02). Cyberspace persistence is the continuous ability to anticipate the adversary's vulnerabilities, and formulate and execute cyberspace operations to contest adversary courses of action under determined conditions (adapted from "persistency" in JP 1-02).

capabilities, and counter attacks close to their origins. Continuous engagement imposes tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks. We will pursue attackers across networks and systems to render most malicious cyber and cyber-enabled activity inconsequential while achieving greater freedom of maneuver to counter and contest dangerous adversary activity before it impairs our national power.

Through persistent action and competing more effectively below the level of armed conflict, we can influence the calculations of our adversaries, deter aggression, and clarify the distinction between acceptable and unacceptable behavior in cyberspace. Our goal is to improve the security and stability of cyberspace. This approach will complement the efforts of other agencies to preserve our interests and protect our values. We measure success by our ability to increase options for decision makers and by the reduction of adversary aggression.

Commander's Intent

Our purpose is to achieve cyberspace superiority by seizing and maintaining the tactical and operational initiative in cyberspace, culminating in strategic advantage over adversaries. Our efforts will increase our freedom of maneuver, create friction for adversaries, and cause them to shift resources to defense. We will erode their belief that hostile activities in cyberspace against the United States and its allies are advantageous. We will meet the 2018 National Defense Strategy's mandate to hold adversaries accountable for cyber-attacks.

USCYBERCOM will contribute to our national strategic deterrence. We will prepare, operate, and collaborate with combatant commands, services, departments, allies, and industry to continuously thwart and contest hostile cyberspace actors wherever found. We will enable and bolster our partners. We will share our insights in order to anticipate evolving cyberspace threats and opportunities. We will attract new partners and strengthen ties with critical mission partners—particularly the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and the rest of the Intelligence Community.

We will keep policymakers and commanders apprised of cyberspace threats, the operating environment, and changes needed in policies and processes to achieve superiority. We will execute our new responsibilities that accompany elevation to a Unified Combatant Command, emphasizing mission and operational outcomes and enhancing the readiness of the nation's cyberspace military forces.

Imperatives

The following imperatives support this guidance. Our imperatives are mutually supporting, with success in one enhancing success in the others. They dictate what we must do in order to retain the initiative in cyberspace. Attaining and sustaining these imperatives creates uncertainty for our adversaries and makes them hesitate to confront the United States. We must identify obstacles to achieving our goals, develop and implement plans to overcome those obstacles, and establish meaningful metrics to gauge our progress.

IMPERATIVE 1: Achieve and sustain overmatch of adversary capabilities. Anticipate and identify technological changes, and exploit and operationalize emerging technologies and disruptive innovations faster and more effectively than our adversaries. Rapidly transfer technologies with military utility to scalable operational capabilities. Enable our most valuable assets—our people—in order to gain advantages in cyberspace. Ensure the readiness of our forces.

IMPERATIVE 2: Create cyberspace advantages to enhance operations in all domains. Develop advantages in preparation for and during joint operations in conflict, as well as below the threshold of armed conflict. Integrate cyberspace capabilities and forces into plans and operations across all domains.

IMPERATIVE 3: Create information advantages to support operational outcomes and achieve strategic impact. Enhance information warfare options for Joint Force commanders. Integrate cyberspace operations with information operations. Unify and drive intelligence to support cyberspace operations and information operations.

Integrate all intelligence capabilities and products to improve mission outcomes for the Joint Force and the nation.

IMPERATIVE 4: Operationalize the battlespace for agile and responsive maneuver. Facilitate speed and agility for cyberspace operations in policy guidance, decision-making processes, investments, and operational concepts. Ensure every process—from target system analysis to battle damage assessment, from requirements identification to fielded solutions, and from initial force development concepts to fully institutionalized force-management activities—aligns to the cyberspace operational environment.

IMPERATIVE 5: Expand, deepen, and operationalize partnerships. Leverage the talents, expertise, and products in the private sector, other agencies, Services, allies, and academia. Rapidly identify and understand cyberspace advances wherever they originate and reside. Increase the scope and speed of private sector and interagency threat information sharing, operational planning, capability development, and joint exercises. Enable and bolster our partners.

Risk Mitigation

The approach described in this document entails two primary risks. The first concerns the employment of a high-demand, low-density maneuver force. The prioritization of highly capable states and violent extremists means the Command will devote comparatively fewer resources and less attention to other cyber actors. The Command will seek to mitigate this risk indirectly by increasing resiliency in DOD systems against all threats in order to render most malicious activity inconsequential, and directly by sharing intelligence and operational leads with partners in law enforcement, homeland security (at the federal and state levels), and the Intelligence Community.

The second risk is diplomatic. We recognize that adversaries already condemn US efforts to defend our interests and allies as aggressive, and we expect they will similarly seek to portray our strategy as "militarizing" the cyberspace domain. The Command makes no apologies for defending US interests as directed by the President through the Secretary of Defense in a domain already militarized by our adversaries. To the maximum extent possible, we will operate in concert

with allies and coalition partners. We will also explain to oversight entities and the public the nature of threats in cyberspace, the threatening conduct of our adversaries, the limitations of passive defenses, and our scrupulous regard for civil liberties and privacy.

Mitigation of these primary risks will occur in parallel with the Command's assumption of unified combatant command status and, if directed, its conditions-based approach to termination of the current dual-hat command relationship with the NSA. Regardless of whether, when, or how the "dual hat" terminates, however, we will adopt a comprehensive risk management approach to maintain synergy between operational objectives and the intelligence required to inform and sustain effective cyberspace operations.

Implementation

This guidance informs our operations, structure, and resource requirements. The Functional Campaign Plan for Cyberspace operations (FCP-CO) constitutes the implementation plan for this guidance. The FCP-CO is a living document requiring regular updates to reflect changes in priorities, doctrine, capabilities, and the operating environment. The FCP-CO Assessment is the process for assessing implementation, and for discovering, validating, and approving changes to drive continuous improvement. The USCYBERCOM Chief of Staff will oversee the assessment function, and all campaign plan assessments are to be reported to the USCYBERCOM Commander.

The key to success is execution, and everyone has a part in this effort. Each Service cyber component, Joint Force headquarters, and staff directorate should embrace this guidance, communicate it to the workforce, work to implement it, and ensure all personnel understand their role and functions—all the while providing direct feedback on the effectiveness of its execution.

The monograph looks at how major powers have tried to pursue three objectives in cyberspace, viz. (1) strengthening or enhancing national cyber defences, and (2) striving to shape the international cyber environment by leveraging economic and technological capabilities, and (3) through defining and evangelising international cyber norms. A section on the cybersecurity preparedness of the countries of the South Asian region is incorporated to highlight those vulnerabilities and deficient capacities and capabilities that give the major powers a foothold to pursue their objectives.

Dr. Cherian Samuel is Research Fellow in the Strategic Technologies Centre at the Manohar Parrikar Institute for Defence Studies and Analyses. He has written on various cyber security issues, including critical infrastructure protection, cyber resilience, cybercrime, and internet governance. His current research areas include the role of the military in cybersecurity.

MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

Manohar Parrikar Institute for Defence Studies and Analyses

No.1, Development Enclave, Rao Tula Ram Marg,
Delhi Cantt., New Delhi - 110 010
Tel.: (91-11) 2671-7983 Fax: (91-11) 2615 4191
Website: http://www.idsa.in