Militaries in Cyberspace
Approaches, Expectations and Outcomes

Cherian Samuel[*]

Militaries are the sword arm of the state, entrusted with defending the state against all threats that would harm its interests. These threats are increasingly emanating from cyberspace and militaries around the world are being called upon formally to undertake responsibility for defending against threats from this domain in addition to the existing physical domains of land, sea, air and space. The unique nature of this domain has required some restructuring on the part of the military. This has led to its own set of complications when it comes to re-alignment of organisation, recruitment of personnel, and working with other actors in the civilian space. This article looks at the cyber force structures in a number of countries to draw out the underlying logic behind the creation and modifications that the military in particular has gone through over a period of 10 years. It looks at the initial approaches, the expectations behind those approaches, and the eventual outcomes.

Keywords: *Cyberwar, Cybersecurity, Military Restructuring, Cyber Command*

Over the years, many countries have found themselves in a constant contestation in cyberspace with adversaries and a variety of hostile actors with different goals, varying skills, resources and determination. The latter are helped in their efforts by a lack of focus on the part of governments, the widely scattered skills in various parts of the government, overlapping areas of responsibility, and indifference at the highest levels on ways to tackle these threats brought about by ignorance of the extent

[*] Dr Cherian Samuel is a Research Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), New Delhi.

ISSN 0976-1004 print

Journal of Defence Studies, Vol. 17, No. 1, January–March 2023, pp. 5–24

of the threat and its rapidly changing character. Added to this is the fact that cyberspace was not constructed with security in mind, but has rather been bolted on subsequently. The issue of attribution has also been a major impediment to identifying and going after the bad actors and it is unlikely to be resolved unless the web is reconstituted fundamentally. Malicious actors have taken advantage of all these factors to carry out both tactical and strategic operations in cyberspace.

Countries around the world have been engaged in a long-drawn out and often torturous process of creating and re-aligning frameworks to respond to cyber threats. This includes creating new organisations, synergising existing organisations and building up capacities to respond to the ever-burgeoning threats and threat actors. At the same time, they also have to take into account emerging technologies related to the domain which are inherently dual-use in nature, and also make short, medium and long term threat assessments on the impact of these new technologies to the existing threat scenarios. The role of the military in addressing these new threats is yet to be figured out, partly because the lead role in responding to these threats is largely taken up by the intelligence agencies that often prefer to operate in the shadows and zealously guard their turf.

The military has an important role to play in responding to cyber threats because of certain inherent characteristics, which makes it most suitable to form a comprehensive response. In the first instance, the nature of the organisation itself with a number of agencies offering different competencies have had to be fused together for a comprehensive response to such threats. From just fulfilling an offensive and defensive role, today's militaries are expected to provide a range of responses depending on the threat perception as well as the capabilities and capacities of the enemy. But the militaries face their own sets of complications when it comes to re-alignment of organisation, recruitment of personnel, and working with other actors in the civilian space.

Beyond the general policies in cyberspace, this article looks at the cyber force structures in a number of countries to draw out the underlying logic behind the creation and modifications that the military in particular has gone through over a period of 10 years. It looks at the initial approaches, the expectations behind those approaches, and the eventual outcomes.

A study of how the military is conceptualising the cyber-environment, how it is being re-shaped by the cyber domain and the manner in which this is happening is quite relevant, so as to avoid the pitfalls other countries struggled with in the past. The US military's concept of Revolution in Military Affairs (RMA) and the resultant Network Centric Warfare, which was put to use during the first Gulf War, was analysed in great detail by the Chinese military as the country formulated its strategy and doctrines for engagement in cyberspace. This playbook was also followed by the Russians as they took advantage of the unique nature of cyberspace to not only formulate an agile doctrine utilising the capacities available to them, including non-state actors, but also took the battle into the US cyberspace. The US took many steps that ultimately resulted in the establishment of the US Cyber Command, though the main trigger was a massive breach of US military networks in 2008. However, it has taken about 10 years for the US to bring its strategic doctrines in line with the challenges it is facing in cyberspace. As the Indian military is embarking on building a presence in cyberspace, it would be prudent to analyse the approaches of various powers and the challenges they faced in amalgamating and aligning their assets to have a credible and proactive presence in cyberspace.

The countries chosen for this study are the United Kingdom (UK), Israel and Russia, all of which are major cyber powers in their own right. However, they have all had differing approaches, expectations and outcomes, based on their priorities, and the broader geo-political environment and requirements of their political masters. Historical legacies also seem to have played a big role in framing their approaches.

Underpinnings of UK's Cyber-posture and Strategy

The UK has a long history of trying to frame cyber strategies that account for the threats faced in cyberspace without unduly constraining the scope for technological innovation and societal advancement it offers. The UK's cyber-posture flows from the national security strategies that have been released over the years. The first national security strategy to mention cyber was the one in 2008, which raised the possibility and threat of cyberattacks. In 2009, the Cabinet Office adopted its first cyber security strategy which placed emphasis on the safety, security, and resilience of cyberspace to be seen in conjunction with the opportunities it provided. This is the broad template around which the overall cyber strategies have been framed. There was a steady and increasing emphasis on cyber threats, subsequently, with the UK Cyber Security Strategy, *Protecting and Promoting the UK in a Digital World*, released in 2011.

A year earlier, the UK Strategic Defence and Security Review had been published in 2010, which established a four-year National Cyber Security programme that provided for an investment of 650 million GBP to be distributed among various organisations that played a vital role in cyber security. An additional 210 million pounds was provided in 2013 for raising awareness and skills and standards. The government also established a robust feedback loop in place that kept a watch on the implementation of objectives outlined in these documents. In a 2016 ministerial statement, the following broad principles were outlined as the goal of British cyber security strategy:

1. Make the UK one of the most secure places in the world to do business in cyberspace.
2. Make the UK more resilient to cyber attack and better able to protect its interests in cyberspace.
3. Help shape an open, vibrant and stable cyberspace that supports open societies.
4. Build the UK's cyber security knowledge, skills and capability.[1]

UK's Conceptualisations of the Threats from Cyberspace

The 'Cyber Primer' brought out by the UK Ministry of Defence laid it all out very succinctly; the rapid expansion of cyberspace and its extension into every aspect of human existence had made it very attractive as a means of identifying and locating vulnerabilities which could be exploited in and through the online space. For countries that were intent on using this medium to benefit their citizens, organisations, private sector enterprises and in governance, there was an urgency in finding ways to mitigate, if not overcome, these threats. The size of the threat surface made it a very difficult task, particularly because virtually the same networks were used by consumers ranging from individual to private organisations, the government and even the military. Therefore, the threats also could have a serious impact on government, economic, military and industrial well-being of the nation.

While intelligence agencies, particularly those tasked with communications intelligence or *comint* such as the Government Communications Headquarters Agency (GCHQ), have been at the forefront in responding to the cyber threats, there is a tendency on their part to favour offensive and intrusive actions over defence. Hostile actors targeted military networks in order to: (a) seek out intelligence about UK military plans; (b) steal intellectual property and intelligence on

UK military capabilities; (c) exploit UK military capabilities using their military and intelligence services with knowledge of the vulnerabilities; (d) deny the UK use of its cyberspace communications channels; (e) conduct subversive activities using their intelligence services; and (f)use proxies or large numbers of synchronised and coordinated partisans to cover the true origin of their activities within cyberspace.[2]

In an era of persistent competition, the military, therefore, has had to formulate a response centred around persistent engagement.[3] The UK has tried to encapsulate its response through various doctrines and approaches, including the fusion doctrine, the integrated approach and the full spectrum approach. All of these envisage a role for the military both in terms of its existing role as security provider as well as a specific cyber role. As the sword arm of the state, the military is given the right to use force in accordance with international law in much the same way as the right to exercise violence is the monopoly of law enforcement agencies under domestic law. Militaries having cyber capacities give a broader range of options to governments to respond to threats appropriately. Those militaries that have integrated jointness in their system are also better placed to lead cyber responses during a time of conflict, since they already have experience with coordination across various functions. With the United Nations having agreed that existing international laws apply in cyberspace, militaries are also better placed to apply standards of distinction and proportionality and discrimination, and frame rules of engagement, if at all possible, in cyberspace.

Another major reason given for having a clearly delineated cyber role is to encourage military personnel to incorporate cyber into their activities. Cyber operations, currently a niche area, is expected to be mainstreamed rapidly as militaries operate in and through the cyber domain in conjunction with the other domains of maritime, land, air and space. Mainstreaming cyber in the military will increase cyberspace awareness, agility and utility by generating warfighters capable of operating in cyberspace based on a thorough understanding of the domain rather than simply producing keyboard cyber warriors.[4] It would also go some way towards ameliorating another issue faced by militaries as they modernise, that of coordinating between hitherto separate and autonomous or standalone teams within the military ecosystem. In the case of cyber, this would include teams operating electronic warfare systems, signal intelligence and those running the communication and information systems. There has to be an understanding of every function of each of these teams in order to facilitate closer integration and interaction. Militaries are also not used to coordinating outside of their domain, whereas cyber command and control requires close coordination with multiple agencies and even with multiple countries. In addition to this, they also need to coordinate with the private sector which further complicates issues since there are also matters of secrecy to be sorted out.

The threats to the military are seen not only to its own immediate networks but also to that of suppliers, i.e., the defence industrial complex sub-contractors in the procurement, logistics and support areas. They are in fact vulnerable because they exist even in the form of small medium companies which usually do not have the bandwidth to invest adequately in cyber security, and thus face attacks regularly. The interdependencies of critical information infrastructure means that attacks may not only come from unexpected quarters, but can also lead to unexpected impacts.[5]

Notwithstanding this, the greatest difficulty faced by militaries is to decide their role inside this space. Policy-makers and strategists have tried to resolve this conundrum using the method of thinking of boundaries in concentric circles, or in the case of the UK military as near, mid and far operating spaces. The 'near' comprises networks and systems that are directly controlled, 'mid' comprises those networks and systems that are critical infrastructure but not under the direct control of the military or other state agencies, and 'far' comprises networks and systems that are owned by third parties that could even be outside the country.[6] Though this method sounds good in theory, in reality, civilian and military cyber infrastructure cannot be delineated and often overlap. Nonetheless, it provides a basic frame of reference for conceptualising the role of the military in cyberspace.

Agencies

At the apex level, the responsibility and accountability for cyber security was with the Home Office, however the increasing need for coordination led to it being shifted to the Cabinet Office. Within the Cabinet Office, cyber security is under the National Security Council Secretariat with coordination being carried out by the office of Cyber Security and Information Assurance.

In 2015, the combined National Security Strategy and Strategic Defence and Security Review officially declared that it would be the responsibility of the Government Communications Headquarters

(GCHQ) to 'develop capability to detect and analyse cyber threats, pre-empt attacks and track down those responsible'.[7] The GCHQ has been in the business of signals intelligence since 1919 and has sustained its leadership position and capabilities over the years. Historically, the GCHQ reported to the Secretary of State for Commonwealth and Foreign Affairs with its primary clients being the Ministry of Defence (MoD), the Foreign and Commonwealth Office, and law enforcement agencies and intelligence agencies, including the MI5 security service and MI6 Secret Intelligence Service. It was estimated to have a staff of over 5,000 and the lion's share of the single intelligence budget which was approximately 2.2 billion GBP in 2021. Though its actions were kept secretive, among the few acknowledged ones included a 'major offensive cyber campaign' against ISIS in partnership with the MoD.[8]

John Ferris, official historian of the GCHQ and author of the book *Behind the Enigma: The Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency* noted that for the first time in its history, GCHQ was responsible for a major fighting threat and had become a fighting service in its own right. If in 1938, the ratio of soldiers to signal intelligence personnel was 200 to 1, by 2020, the ratio had become 14 to 1. The shift in its role and its increasing visibility meant that it also had to transform from a secretive intelligence agency to more public facing entity. To this end, the National Cyber Security Centre (NCSC) was established, largely inspired by Israeli efforts to fashion a nurturing ecosystem. Thus, even as the parent organisation was tasked to share information with the private sector, both organisations were also mandated to place emphasis on research and development. Encouragement of start-ups was through the establishment of a cyber accelerator which provided access to GCHQ technology capabilities to those companies that were selected to be a part of this accelerator. GCHQ was also involved in training cyber security professionals, identifying young talent starting from the school level and even a GCHQ certified master's degree in cyber security.[9] Despite these efforts, the NCSC had to make enormous efforts to overcome the perception that it was into surveillance, and portrayed itself as more of a bobby on the beat trying to get Britain's cyber security into shape.

The military also had to be plugged into this space since it was in the crosshairs of hostile actors for the reasons mentioned earlier. A joint cyber group was created to integrate the capabilities within the MoD primarily to defend its networks but also to assist other agencies when the need arose.[10] The joint forces' cyber group created in 2013 had two separate joint cyber units with defensive and offensive capabilities, respectively. These were the Joint Cyber Unit (JCU) Cheltenham and JCU Corsham, with the former in charge of offensive operations and the latter, defensive operations. The MoD Joint Doctrine Note (JDN) 1/18 on Cyber and Electromagnetic Activities released in 2018 described cyber operations as 'the planning and synchronisation of activities in and through, cyberspace to enable freedom of manoeuvre and to achieve military objectives', and cyber operations were categorised into four distinct roles: offensive cyber operations; defensive cyber operations; cyber intelligence, surveillance and reconnaissance (ISR); and cyber operational preparation of the environment.[11]

The first step towards synergising the capabilities scattered across the military began with the establishment of the Force Troops Command (FTC), 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 and HQ West Midlands and 77th Brigade. In 2019, the Force Troops Command was renamed as the 6th Division.

In November 2020, the National Cyber Force (NCF) was established, with personnel drawn from GCHQ, MoD, the Secret Intelligence Service (SIS/MI6) and the Defence Science and Technology Laboratory (DSTL), with the units' funding coming from the MoD. The NCF brought together all the personnel into a single organisation under unified command to cover the full range of the UK's national security priorities—from tackling serious criminality to preparing for war. 'As such, it has no equivalent anywhere else in the world.'[12] The justifications given for the creation of NCF are many and varied, from rationalising the use of scarce personnel to giving real world experience to the military, to ensuring closer integration between defence and offence.[13] Some of the questions raised about the focus of this hybrid organisation are: Is it taking down the infrastructure of ransomware cybercriminals; counter-cyber operations against hostile state actors; or preparing for and engaging in military operations? The 2022 National Cybersecurity Strategy stated that the UK would 'make more routine use of the NCF's capabilities to disrupt threats from both state and non-state actors and to support the UK's wider national security interests', which seems to indicate a more aggressive role that could lead to more instability, rather than less instability in cyberspace. This is in conflict with the UK's declared preference for undertaking only lawful activities in cyberspace.

Underpinnings of Israel's Cyber-posture and Strategy

In the case of Israel as well, its history and surrounding environment have shaped its military's response to cyber threats. It has been perpetually in a state of heightened readiness since it is surrounded by hostile neighbours. The advent of cyberwarfare has presented new challenges to Israeli policy-makers, but they have seized upon it as an opportunity to build on Israel's strengths in technology and their application in the military to become world leaders in utilising cyber to augment the traditional strengths of the military.

The threats facing Israel following the big wars of 1960s and 1970s have generally been hybrid security threats. They have ranged from conventional low intensity and asymmetrical threats from various groups to threats at the regional level, even in the form of weapons of mass destruction, missiles, and now cyber threats. Most of these threats have been sought to be countered through deterrence and retaliation. The advent of cyber threats has resulted in new security uncertainties and challenges.

Israel's Conceptualisations of Cyberspace

Most analysts believe that Israel's cybersecurity policy has drawn inspiration from its strategic policy which can be traced all the way back to the doctrine and principles enunciated by David Ben Gurion, its founding father and first Prime Minister. The principles he enunciated for the defense forces focused on: (i) the defence of the state, (ii) its infrastructure and interests, (iii) deterrence against potential attacks, (iv) forming alliances with great powers, and (v) development of sophisticated early warning capabilities to compensate Israel's lack of strategic depth.[14]

Considering these points, Israel formulated a concentric circle of military commitments, these being the 'immediate perimeter', 'intra frontiers', and 'remote commitments'. With the expansion of cyberspace and its permeation into virtually every sphere of political, military and socio-economical spaces, the future battlefield comprising cyber and information technologies was also recognised as a new area of concern. Adversaries seized upon the advantages these domains provided for asymmetric warfare, where they could attack critical infrastructure without the fear of being attacked in return, particularly given the existing problems of attribution and low numbers of counter-value targets. Israeli policy-planners also recognised that since it was in a state of perpetual conflict unlike other countries, this would also reflect in cyberspace. The pattern of periods of peace regularly punctuated by military operations on the periphery followed by retaliation meant that a similar ebb and flow would be expected in cyberspace.[15]

On the military side, there were attempts to do a comprehensive reorganisation and create a unified cyber command. The existing organisations within the military comprised of the Telecommunications Directorate responsible for cyber defence and the Signals Intelligence Unit of the Directorate of Military Intelligence which was 'responsible for intelligence collection and foreign cyber operations'.[16] However, that plan was shelved for reasons that are unclear. The Israeli defence forces also brought out a public defence doctrine in 2015 which incorporated cyber into the overall strategy, effectively declaring cyberspace as the 5th domain of warfare.[17] Quite comprehensive for its time, the strategy looked at cyber in its role as a support function, as well as for offensive and defensive purposes 'at all levels of combat (i.e. strategic, operative, and tactical)'.[18] Creating capacities equally in all these areas was seen as essential to 'the functioning of the state and IDF institutions, the utilization of intelligence, collective defence, influence operations, and achieving legitimacy as well as legal responses, as well as maintaining a credible deterrence posture in cyberspace'. This venture in 2015 provided the staging point for the military for 'developing new operational concepts, methodologies and technologies for shortening the sensor to shooter cycle, intelligence threat analysis and target creation, early warning and absorption readiness, and active defence command and control'.[19] However, the main goal of creating a Cyber Command was still borne even though it was announced by the then Chief of General Staff Gadi Eizenkot.

However, the national cybersecurity strategy of 2017 laid out the defensive and offensive responsibilities of the Israel Defense Forces (IDF). The doctrine was based on the overall guiding principles that have guided Israel's defence since its inception, including deterrence, ensuring decisive victory, early warning and alliances. Whilst some elements of the overall doctrine have been incorporated into the cyberdoctrine, others are not so easy to incorporate. For instance, deterrence would call for immediate tit-for-tat actions, but it has proved to be an exception than the norm since cyber attacks are too numerous to entail a continuous response. Thus, the emphasis seems to be more on developing and optimising capabilities for a flexible response, with gradations based on explicitly mentioned enemies and threats, as well as whether those threats are manifesting in times of relative peace or enhanced hostility, given the relatively volatile situation in that part of the world. In peacetime, the Israel National Cyber Directorate (INCD) is in charge of managing national cyber defense. During times of emergencies, the IDF coordinates offensive and defensive cyber campaigns at the national level.[20] Whether this framework will stay viable or there will be another attempt towards creation of a Cyber Command remains to be seen.[21]

Agencies

The main agencies responsible for defensive and offensive cyber operations have been the internal security agency, Shin Bet and the National Intelligence Agency, Mossad. A number of agencies have been established on the civilian side, starting with the National Cyber Bureau (NCB) as a coordinating agency in the Prime Minister's Office in 2012. At that time itself, there was opposition to its establishment with Shin Bet, the internal security agency, claiming that the NCB would be unable to carry out its mandate because it lacked intelligence-gathering capabilities, had no operational tradition and little possibility of integration with similar security organisations worldwide.[22] The establishment of other agencies subsequently, including the National Cyber Security Authority (NCSA) in 2015, and merging of NCSA and NCB into the INCD in 2018 point to continued turmoil over the respective areas of authority of all these agencies. Amongst the mandates of the INCD was to create coordination mechanisms with the military and to come up with unified threat projections to 'improve situation analysis capabilities for intelligence services and stakeholders'.[23] Even though the INCD had the responsibility for coordination at the national level, that role was to be taken over by the Israeli Defence Forces during times of war or national emergency.[24]

The creation of the INCD has still not addressed the underlying tensions over distribution of responsibilities. According to an ETH Zurich study, 'even though on paper the INCD is the central and most powerful agency, cooperation with other agencies is often challenging, especially with the older and more established agencies such as Shin Beth'.[25] At the same time, giving a dominant position to the intelligence agencies in a democracy is not sustainable in the complex cyber environment since they have much lower levels of oversight and responsibility. Nevertheless, Shin Bet and Mossad continue to conduct cyber operations independently, while sharing information and expertise, when and where required. 'This is why no public information is available on their cybersecurity-related tasks, actions, operational capabilities, and cooperation links with other agencies'.[26]

The Central Collection Unit of the Intelligence Corps or Israeli SIGINT National Unit (ISNU), more commonly known as Unit 8200, is responsible for offensive cyberwarfare. Though not much is known about it, the operations it has undertaken are well-known, through the malware created for those operations and subsequently analysed by cybersecurity specialists. The most famous of these was Stuxnet followed by Duqu, Flame and Gauss malware.

These malware could be created because Unit 8200 was backed up by virtually unlimited resources and given *carte blanche* to engage in sabotage of enemy industrial facilities, carry out cyber espionage and undertake other actions in support of the military forces. According to estimates, the unit has about 5,000 personnel and is the largest unit in the IDF.[27] It has also benefitted from a close association with the US National Security Agency (NSA) which gives it access to the information collected through its worldwide signal intelligence collection network. Collaboration is not just limited to data sharing but also technical know-how, and 'information on access, intercept, targeting, language, analysis and reporting'.[28]

The notable aspect about Israeli efforts towards becoming a leading power in cyberspace is the role the military played in this endeavour, which other countries have also tried to emulate without much success though, since some attributes are unique to Israel. The cyber ecosystem evolved because Unit 8200 took advantage of the four-year compulsory military service for Israelis to select promising students based on their analytical capabilities and train them in cyber technologies. Many of these youngsters then went on to work or found cyber-security start-ups, leading to Israel being given the moniker of start-up nation.[29] The IDF can also call on them when required, for a mandatory reserve duty for up to three weeks every year until the age of 50.[30] A final point in favour of the success of this ecosystem is that the passouts from the military system maintain a social network that creates strong links between the private and public sector, military, and intelligence community.[31]

The military's influence on cyber policy also comes in through the appointment of former IDF officers with operational experience in cyber to the top posts in the INCD. Eviatar Matania, the founding Director of both the NCB and the INCD, had worked in the IDF as well as in the private sector. His successor Buky Carmeli was also a former head of the M.O.D. cyber and technology defense authority. He was succeeded by Yigal Unna, who had not only served in Unit 8200 but also in the Shin Bet as head of its cyber warfare unit. The current head, Brigadier General Gaby Portnoy (Retd), served 31 years in military intelligence, including as the Head of Operations in the Intelligence Corps.[32]

Underpinnings of Russia's Cyber-posture and Strategy

Russia's approach towards cyber-conflict is seen to be conditioned around a number of factors, including the historical legacies and strategies developed through many decades of waging information war. Russia's focus has been on securing its cyberspace from the threat of information warfare and cyber weapons being used against it by external powers, while at the same time retaining control over domestic cyberspace. The Russians, in fact, club cyber war and information war together, believing them to be two sides of the same coin. 'In keeping with traditional Soviet notions of battling constant threats from abroad and within, Moscow perceives the struggle within "information space" to be more or less constant and unending'.[33] The internet, and the free flow of information it engenders, is viewed as a threat as well as an opportunity in the sense that while the domestic arena must be protected against attempts at disinformation and destabilisation, it provides Russia the chance to do the same to hostile powers.[34] Russian military theorists conceptualised information warfare as comprising the whole of computer network operations, electronic warfare, psychological operations and information operations.[35] The articulation of this was through the so-called Gerasimov Doctrine, based on a speech by General Valery Gerasimov, then Chief of Army Staff before the Russian Academy of Military Sciences in February 2013, followed by an article in a military journal wherein he said, 'Information confrontation opens up wide asymmetric opportunities to reduce the enemy's combat potential'.[36] To this end, Russia has been an active player in cyberspace, realising early on that it could be used to serve its national purposes particularly when it came to moulding the neighbourhood, which had been volatile ever since the fallout of the Soviet Union. The first inkling of this came during the war with Georgia in 2008 when information and influence operations played a big role. However, most of the activities were done by the intelligence agencies, with the military sticking to its traditional role as a conventional army.

According to Andrei Soldatov and Irina Borogan, the Russian military, which experienced a sharp drop in budget allocations in the 1990s and a corresponding decline in prestige, did not have much say in cyber affairs until 2013 when the Ministry of Defence announced plans to create 'cyber troops'.[37] The growing overlap between internal and external operations necessitated a changeover from the informal arrangements to a more formalised division of labour. This is also reflected in the large number of strategy documents related to cyber, including the National Security Strategy (2015), Foreign Policy Concept (2016), Information Security Doctrine (2016), and Conceptual Views on the Activity of the Armed Forces in the Information Space (2016).

Russia's Conceptualisations of Cyberspace

The misunderstandings over Russian activities in cyberspace are said to have arisen from the proclivity of analysts to look at Russian activities through a US lens, i.e., based on US perceptions of the cyber domain. While some analysts say that Russia has a better conceptualisation of cyberwarfare as a grand strategy as opposed to thinking about it purely in tactical terms,[38] the opposite perspective could also be true, i.e., Russia approaches cyber largely in tactical terms. This would seem to be the case if one purely looks at Russia's actions in terms of cyber operations. However, they seem more strategic when the entire gamut of operations is taken into consideration. According to Janne Hakala and Jazlyn Melnychuk, 'information confrontation' is a more appropriate term to use than 'information warfare' since Russia views this as a constant struggle as opposed to the Western delineation of war and peace being two binaries. The Russian Ministry of Defence describes information confrontation as 'a clash of national interests and ideas, where superiority is sought by targeting the adversaries' information infrastructure while protecting its own objects from similar influence'.[39]

Russia has been coming out with information doctrines since 2000, which have codified Russia's view on information threats. The 2000 doctrine provided a broad definition of the information sphere, which is a 'combination of information, information infrastructure, entities involved in the collection, generation, distribution and use of information, as well as a system for regulating the resulting public relations'.[40] Russia's Ministry of Defence 2011 Concept on the 'Activities of the Armed Forces of the Russian Federation in the Information Space' provided a clear definition of information warfare: 'the confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilise the state and society, as well as coercing the state to take decisions for the benefit of the opposing force'.[41] The basic thrust of these doctrines has been to push the line that Russia is at the receiving end of continuous attacks aimed at destabilising it. The 2016 doctrine called for a more muscular response incorporating 'strategic deterrence and prevention of military conflicts that may arise as a result of the use of information technology; forecasting, detection and assessment of information threats, including threats to the Armed Forces of the Russian Federation in the information sphere and neutralisation of information psychological impact, including aimed at undermining the historical foundations and patriotic traditions associated with the defense of the Fatherland'.[42]

The overwhelming thrust on victimhood and being the subject of attacks provides a clue as to why Russia, on the one hand is at the forefront to push forward rules of the road and even treaties in cyberspace, at the same time it continuously violates virtually every principle it propagates. This dichotomy between what the Russian state says and actually does is one of convenience. 'The continuous omission of an official endorsement of offensive cyber capabilities in its doctrine allows the Russian government to claim plausible deniability and maintain a narrative of a defensive power under threat by an aggressive West'.[43]

Agencies

Of the state agencies active in this domain, the biggest is the Federal Security Service (FSB) largely viewed as the successor to the Komitet Gosudarstvennoy Bezopasnosti (Committee for State Security or KGB). The GRU (Main Directorate of the General Staff of the Armed Forces of the Russian Federation) is the military external intelligence agency. Both these organisations have been engaged in cyber operations, but the extent of their involvement has largely depended on the nature of Russia's conflicts with other countries. The FSB is charged with internal security, which is why it had developed relations with Russian hackers from the early 1990s. Russia's wars with Georgia and Estonia also saw the FSB playing a leading role since it had existing intelligence apparatus in these two countries, which were part of the former Soviet Union.

Despite kinetic warfare taking place, especially in the case of Georgia, the GRU, which was the military intelligence service, was largely confined to providing traditional intelligence in as a direct support to the military.[44] The GRU came back into play after the North Atlantic Treaty Organization (NATO) began to focus on cyber and began to coordinate more amongst member countries on cyber. Growing US capabilities and announced intentions to shift more responsibility of cyber operations to the military was another contributing factor. This was evident by actions following the establishment of the US cyber command in 2009. The GRU started receiving attention and resources from 2013 as part of the attempts by Russia's Ministry of Defence to improve and advance the militaries' research and development on cyber operations, signals intelligence and electronic warfare.[45] The 2014 military doctrine listed 'development of forces and means of information confrontation' as one of the main tasks for equipping Russia's armed forces for the 21st century.

Hakala and Melnychuk succinctly sum up the evolution of the main cyber actors in Russia thus:

> The actors and agencies involved in Russia's cyber operations evolved alongside Russia's perception of modern warfare and the threats posed by Western use of information technologies to further its military and foreign policy goals. In the first decades of the post-Soviet period, the FSB had a primary role in conducting cyber operations alongside the support of independent Russian hackers. Around the same time, a consensus formed among Russia's elite that warfare includes military and non-military measures during peace and wartime, and Russia's Defense Ministry increased its efforts to establish an organized and centrally controlled cyber force. These changes, coupled with the operational opportunities presented by Russia's intervention in Ukraine, enabled the GRU to adopt a leading position in offensive cyber operations, bringing a historical penchant for risk-taking and aggression to its operations. Additionally, the GRU's traditional command of information operations provided a natural place for cyber alongside information operations – the two core components of information warfare. These realities further enabled the transformation of Russia's strategic cyber operations from seemingly ad-hoc activities to more organized and centrally controlled campaigns that complement Russia's view of modern warfare.[46]

Conclusion

The approaches of the various powers and the challenges they faced in lining up the various facets of cyber into a coherent and functioning framework have been brought out in these case studies. While the theorists and the strategies predicate future conflict based on integration of cyber into the military and call for its quick integration, these case studies show that many obstacles need to be overcome along the way and that the goalposts are always moving. There is no overarching solution or method to achieve these goals, considering not only the complexity of the cyber ecosystem with its multitude of actors, but also because each state, willy-nilly, has had to attempt its own form of trial and error creating new organisations, re-aligning responsibilities and functions, and aligning doctrines and strategies with capacities and capabilities, and more often than not, taking public positions that are at variance with actual actions on the ground. As a case in point, many countries are setting up Cyber Commands and sanctioning offensive operations even though this goes against the international law and existing norms and conventions, and leads to further instability in cyberspace.

The militaries are caught in the crosshairs of the contradictions in policies, all the while expected to have cyber expertise ready at hand, to have incorporated it into their doctrines and be ready for cyber conflict. However, their role is yet to be clearly delineated as seen in the questions swirling around the role of the National Cyber Force of Great Britain. Similarly, Russia has also been pilloried for being at the forefront of carving out treaties and norms for cyberspace while flouting many of them to capitalise on its cyber abilities in the course of its many conflicts. Israel swears on deterrence as the touchstone of its efforts to keep the country safe, yet when it comes to cyber conflict, it has realised that neither deterrence by denial nor deterrence by punishment can prevent it. The threat landscape is too vast for effective denial and the attacks are too numerous for a policy of deterrence by punishment.

Nonetheless, the ultimate takeaway from these case studies is that there has to be continuous innovation in doctrines coupled with relentless slicing and dicing of organisations within the military and outside, in order to arrive at an optimum force structure. Militaries need to take the initiative to carve out their roles in the cyberverse instead of having it laid out for them. At the same time, thay have guard against mission creep, taking on responsibilities that are peripheral to their core functions. Defining those core functions is the challenging task ahead for militaries.

Notes

1. 'Final Annual Report on the 2011-2016 UK Cyber Security Strategy', UK Parliament, 14 April 2016, available at http://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Lords/2016-04-14/HLWS652/, accessed on 18 November 2021.
2. 'Cyber Primer: Second Edition', Ministry of Defence, UK, 20 July 2016, p. 32, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160 720-Cyber_Primer_ed_2_secured.pdf, accessed on 15 December 2021.
3. Phil Lester and Sean Moore, 'Responding to the Cyber Threat: A UK Military Perspective', *Connections—The Quarterly Journal*, Vol. 19, No. 1, 2020, p. 40, available at http://connections-qj.org/article/responding-cyber-threat-uk-military-perspective#:~:text=According%20to%20the%20UK%20doctrine,to%20just%20the%20cyber%20domain.
4. Ibid., p. 42.
5. 'Cyber Primer: Second Edition', n. 2, p. 11.
6. Ibid.
7. 'National Security Strategy and Strategic Defence and Security Review', UK Government, 2015, available at https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015, accessed on 12 November 2021.
8. 'Director's Speech at Cyber UK 2018', GCHQ, 12 April 2018, available at https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018, accessed on 18 October 2021.
9. Melissa Hathaway et al., 'United Kingdom Cyber Readiness at a Glance', Potomac Institute for Policy Studies, October 2016, p. 11, available at https://potomacinstitute.org/images/CRI/CRI_UK_Profile_PIPS1.pdf.
10. Ibid., p. 10.
11. 'Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities', Ministry of Defence, UK, February 2018, p. 32, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrin e_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf, accessed on 18 January 2022.
12. Marcus Willett, 'Why the UK's National Cyber Force is an Important Step Forward', The International Institute for Strategic Studies, 20 November 2020, available at https://www.iiss.org/blogs/analysis/2020/11/uk-national-cyber-force, accessed on 18 November 2021.
13. Ibid.
14. 'Israel's National Cybersecurity and Cyberdefense Posture', Report, Center for Security Studies (CSS), ETH Zürich, September 2020, p. 13, available

at https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf.

15. Michael Raska, 'Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy', Policy Report, S. Rajaratnam School of International Studies, Singapore, 2015, p. 3, available at https://www.michaelraska.de/download/Israel's_Evolving%20Cyber%20Strategy_Raska.pdf.
16. Elena Chachko, *Persistent Aggrandizement? Israel's Cyber Defense Architecture*, Aegis Series Paper No. 2002, Hoover Institution, Stanford University, 2020, p. 4, available at https://www.hoover.org/sites/default/files/research/docs/chachko_webready.pdf.
17. 'Israel's National Cybersecurity and Cyberdefense Posture', n. 14, p. 8.
18. Ibid.
19. Michael Raska, 'Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy', n. 15, p. 11.
20. Ibid., p. 13.
21. Ibid.
22. 'Israel's National Cybersecurity and Cyberdefense Posture', n. 14, p. 10.
23. Ibid., p. 10.
24. Dmitry (Dima) Adamsky, 'The Israeli Odyssey toward its National Cyber Security Strategy', *The Washington Quarterly*, Vol. 40, No. 2, 2017, pp. 113–27, available at https://www.tandfonline.com/doi/full/10.1080/0163660X.2017.1328928.
25. 'Israel's National Cybersecurity and Cyberdefense Posture', n. 14, p. 15.
26. Ibid.
27. Sean Cordey, 'The Israeli Unit 8200—An OSINT-based Study', Report, Center fopr Security Studies (CSS), ETH Zurich, December 2019, p. 4, available at https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/389135/Cyber-Reports-2019-12-Unit-8200.pdf?sequence=1&isAllowed=y.
28. Ibid., p. 11, quoting G. Greenwald, L. Poitras, and E. MacAskill, 'NSA Shares Raw Intelligence including Americans' Data with Israel', *The Guardian*, 11 September 2013, available at https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.
29. Gil Baram and Isaac Ben-Israel, 'The Academic Reserve: Israel's Fast Track to High-Tech Success', *Israel Studies Review*, Vol. 34, No. 2, 2019, pp. 1–17.
30. Sean Cordey, 'The Israeli Unit 8200—An OSINT-based Study', n. 27, p. 15.
31. 'Israel's National Cybersecurity and Cyberdefense Posture', n. 14, p. 15.

32. 'Israel Appoints Ex-General as Head of Government Cyber Security', *Reuters*, 20 February 2022, available at https://www.reuters.com/world/middle-east/israel-appoints-ex-general-head-government-cyber-security-2022-02-20/, accessed on 20 February 2022.
33. Michael Connell and Sarah Vogler, 'Russia's Approach to Cyber Warfare', Occasional Paper, Center for Naval Analyses, March 2017, p. i, available at https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf.
34. Ibid.
35. Ibid., p. 2.
36. Valery Gerasimov, 'The Value of Science Is in the Foresight', *Military Review*, January–February 2016, pp. 23–29 (Originally in Russian).
37. Janne Hakala and Jazlyn Melnychuk, 'Russia's Strategy in Cyberspace', Report, NATO Cooperative Cyber Defence COE, June 2021, p. 18, available at https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf.
38. Michael Connell and Sarah Vogler, 'Russia's Approach to Cyber Warfare', n. 33, p. 2.
39. Quoted in Ibid., p. 5.
40. Bilyana Lilly and Joe Cheravitch, 'The Past, Present, and Future of Russia's Cyber Strategy and Forces', 12th International Conference on Cyber Conflict (CyCon), 2020, p. 134, available at https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf.
41. Russia, Ministry of Defence, The Russian Federation Information Security Doctrine approved by the President of the Russian Federation, 9 September 2000 https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle
42. Bilyana Lilly and Joe Cheravitch, 'The Past, Present, and Future of Russia's Cyber Strategy and Forces', n. 40, p. 136.
43. Ibid., p. 139.
44. Michael Connell and Sarah Vogler, 'Russia's Approach to Cyber Warfare', n. 33, p. 11.
45. Ibid., p. 12.
46. Ibid., p. 20.