MP-IDSA Monograph Series
No. 89 January 2025

Evolving Military Roles in Cyberspace

A Five Nation Perspective

Cherian Samuel

MP-IDSA Monograph Series
No. 89 January 2025

Evolving Military Roles in Cyberspace: A Five Nation Perspective

Cherian Samuel

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

ISBN: 978-81-980805-6-1

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: January 2025

Price: Rs. 325/-

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: Pentagon Press LLP
206, Peacock Lane, Shahpur Jat
New Delhi-110049
Tel. (91-11) 26491568, 26490600
Fax: (91-11) 26490600
email: rajan@pentagonpress.in
website: http://www.pentagonpress.in

Contents

Chapter 1

Introduction

Countries around the world have been engaged in a long-drawn out process of creating and re-aligning frameworks to respond to the cyber threat. This multifaceted process has involved the establishment of new organisations, the harmonisation of existing entities, and the enhancement of capabilities to confront the ever-expanding array of threats and threat actors. Simultaneously, governments have had to navigate the landscape of emerging technologies within this domain, which inherently possess dual-use attributes, while also conducting comprehensive assessments to gauge the short, medium, and long-term implications of these emerging technologies on existing threat scenarios.

Over the years, countries have found themselves in constant contestation in cyberspace with adversaries and a variety of other 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, and overlapping areas of responsibility. Furthermore, the inherent design of cyberspace, which prioritized functionality over security, has contributed to this predicament, as security measures were retroactively implemented. Additionally, the challenge of attribution has emerged as a significant impediment in the identification and pursuit of malevolent actors.

The precise role of the military in addressing these emerging threats remains a subject of ongoing deliberation. This ambiguity arises partly due to the predominance of intelligence agencies in spearheading responses to these threats, as historically, they have operated discreetly and zealously guarded their domain of influence. The military assumes a significant and indispensable role in effectively addressing cyber threats due to inherent characteristics that render it particularly well-suited to

provide a comprehensive response. Primarily, the nature of the military organisation itself comprises various agencies that possess diverse competencies, necessitating their integration to form a cohesive response to such threats. Today's military forces are no longer confined to solely fulfilling offensive and defensive roles; rather, they are expected to offer myriad responses that are contingent upon the perception of threats as well as the adversaries' capabilities and capacities.

However, the military encounters its own array of complexities when it comes to reorganising its structure, recruiting personnel, and collaborating with other actors in the civilian domain. These challenges arise due to the intricacies of realigning organisational structures to effectively combat cyber threats, identifying and acquiring the requisite skill sets within the military ranks, and fostering cooperation with external entities in the civilian sphere.

Both the larger strategic community as well as policymakers face the perplexing dilemma of determining the appropriate placement of cybersecurity within the military's overarching framework. It is crucial to recognize that the military is not an end in itself, but rather operates as a means of safeguarding the security of the state. In this capacity, the military assumes the role of constructing itself as a formidable war machine. Over the course of time, the concept of war has evolved into a realm governed by certain rules, acknowledging that the instruments of war must be carefully calibrated to avoid becoming the cause of war. Scholars and theorists have extensively examined these possibilities over centuries, exploring various concepts and theories that examine the influence of the military on power dynamics between States.

In the context of cyber operations, which possess a multifunctional nature wherein the same techniques can be employed for espionage, disruption, and even more destructive attacks, a distinct phenomenon known as the "cyber security dilemma" arises. This dilemma stems from the fact that actions undertaken within the cyber domain can easily be misinterpreted, leading to a dangerous cycle of escalation and response. Additionally, official statements indicating that a cyber attack may prompt a response beyond mere cyber countermeasures, employing any available means, further compound these complexities.

This monograph looks at the role of the military, or lack thereof, by examining the initial approaches of selected countries—United States, China, Russia, United Kingdom, and Israel—towards the military in cyberspace, along with the underlying expectations and eventual outcomes. Each of these countries have been chosen because they have presented different approaches for their militaries in cyberspace. The United States has been the leading cyberpower because of its early adopter status, and the technological prowess of its military. Cyberspace itself could be said to be a by-product of the military's endeavour to create a communication network that could survive a nuclear explosion. China has been steadfast in recognising cyberspace as a new vector that could provide it a decisive advantage in both low and high-intensity conflict and has taken drastic measures to refashion its cyberforces to that end. Russia has gone in a different direction, preferring to obfuscate its actions in cyberspace by employing proxies in an effort to have plausible deniability. Whilst China also has employed non-State actors, they have till now been largely used for espionage purposes. The United Kingdom has leveraged its membership of the Five Eyes network to remain at the cutting edge, and has tried to sell itself as one of the most cyber-secure countries in the world, repeated breaches, notwithstanding. Recognising the need for civil-military fusion in this domain, it has also tried many experiments in creating a hybrid civil-military cyberforce, without much success. While the preceding countries are major powers in their own right, Israel represents a good example of a middle power, which can be counted among the major powers in the cyber arena by virtue of having bootstrapped its technical prowess to become a world leader in cyber technologies. However, conceptualising the role of its military for the cyber age has proved to be problematic, so much so that it has, time and time again, postponed the creation of a cyber command and instead opted to reorganize its existing military commands to better define the roles and missions of its offensive and defensive cyber warfare capabilities. By analysing these cases, the study aims to shed light on the evolving perspectives and practices of States regarding the involvement of their military forces in the realm of cyberspace. The end purpose is to draw out those lessons that would be useful for Indian policymakers and military planners as they seek to empower the Armed Forces cyber defence and cyber offence capabilities.

The Monograph also contains a list of cyber incidents which are presumed to have been carried out against military and strategic targets of each country by State or State-sponsored actors, extrapolated from various databases.

Chapter 2

United States: Pitfalls of being the First Mover

Underpinnings of cyberposture and strategy

The United States has demonstrated an early recognition of the strategic implications of the cyber domain. The creation of this domain itself was rooted in a strategic purpose—to establish a communication medium capable of functioning in the aftermath of a nuclear attack, where electronic devices were expected to be incapacitated by the resulting electromagnetic pulse. Additionally, the realm of Signals Intelligence (SIGINT) and subsequently information warfare had long been acknowledged as integral components of military operations. Over the years, the US military has developed explicit formulations and doctrines concerning information warfare.

The historical context provides a degree of continuity in the United States' approach to cyberspace. However, it also presents challenges as the US military grapples with the need to adapt existing doctrines to effectively engage in warfare within the cyberspace domain. The evolution of warfare to encompass the cyber realm has needed adjustments, requiring the US military to navigate the complexities of incorporating cyber capabilities into their established frameworks. This provided some element of continuity as well as posed problems to the US military as it struggled to adapt existing doctrines to war fighting in and through cyberspace.

The earliest version of the US Department of Defense directive on information warfare 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

> and command and control countermeasures while protecting the integrity of one's own information systems from such attacks.[1]

Subsequently, information warfare was rephrased as *information operations* largely in recognition of the fact that these activities would also take place during peacetime. The US was also trying to maintain a benign presence in cyberspace without drawing too much attention to its capabilities in this domain. Information Operations was further disaggregated into Computer Network Attack (CNA) and Computer Network Defence (CND), together called Computer Network Operations (CNO).

The information warfare aspect further receded into the background as cyber-attacks took centre stage with the increasing use of networked computers and supporting IT infrastructure systems by the military, making it a valuable target for hostile actors who sought to degrade military capabilities by attacking the networks and end-point devices. As a result, the concept of CNO and its intersection with electronic warfare has emerged as a strategic approach for engaging in offensive and defensive activities, including attacking, deceiving, degrading, disrupting, denying, exploiting, and safeguarding electronic information and infrastructure. [2]

The military encountered several challenges in adapting its mindset to the evolving landscape. This was particularly evident in the realm of cyber operations, where both strategic and tactical operations became necessary. Strategic missions entailed longer timeframes and required extensive planning and scenario development before implementation. In contrast, tactical missions were characterised by their reactionary nature and time sensitivity, necessitating swift and immediate responses

---

1 Michael Warner, "Notes on Military Doctrine for Cyberspace Operations in the United States", *The Cyber Defense Review*, 27 August 2015 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 16 September 2020

2 C. Paul, *Information Operations: Doctrine and Practice,* Praeger Publishers, Westport, 2008, p.94.

to emerging situations.[3] Another mission which achieved prominence was that of Computer Network Exploitation (CNE), i.e., espionage, 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." [4]

Conceptualisations of the threats from cyber space

The classified US Presidential Policy Directive (PPD) 20 issued in October 2012 which was leaked by *The Guardian* in June 2013, 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.[5]

As per PPD 20, defensive cyber operations were actions undertaken to defend or protect against "imminent threat or ongoing attack or malicious cyber activity". A defensive cyber operation would not damage or degrade the infrastructure, assets, communication channels or critical information infrastructure of other States. These operations were to be carried out in defence of own networks, infrastructure and cyber assets from any untoward incident or a breach. On the other hand, offensive operations were defined as unilateral efforts by states

---

3 Michael Klipstein and Michael Senft, "Cyber Support to Corps and Below: Digital Panacea or Pandora's Box?" *Small Wars Journal* at www.smallwarsjournal.com/jrnl/art/cyber-support-to-corps-and-below-digital-panacea-or-pandora%E2%80%99s-box. Accessed on 20 October 2020

4 Ibid.

5 White House, "Presidential Policy Directive 20", *US Cyber Operations Policy,* October 2012 at http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text Accessed on 13 October 2020

to inflict damage to other States' infrastructure or degrade it severely, if the need to do so arises. PPD 20 defined 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". Offensive cyber operations were also to play a role as a deterrent and prevent misadventures by other States viewing cyber as a cost-effective means of inflicting damage on the United States.

Even as recently as the 2017 National Security Strategy, it was recognised that defence was more important than offence in the overall scheme of things. The Strategy stated:

> For most of our history, the United States has been able to protect the homeland by controlling its land, air, space, and maritime domains. Today, cyberspace offers state and non-state actors the ability to wage campaigns against American political, economic, and security interests without ever physically crossing our borders. Cyberattacks offer adversaries low cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our federal networks, and attack the tools and devices that Americans use every day to communicate and conduct business. Critical infrastructure keeps our food fresh, our houses warm, our trade flowing, and our citizens productive and safe. The vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication."[6]

It went on to state:

> Cyberattacks have become a key feature of modern conflict. The United States will deter, defend, and when necessary, defeat

---

[6] US Department of Defense, *National Security Strategy* 2017, 17 December 2017, p.12 at https://history.defense.gov/Portals/70/Documents/nss/NSS2017.pdf?ver=CnFwURrw09pJ0q5EogFpwg%3D%3D Accessed on 14 January 2021

> malicious actors who use cyber space capabilities against the United States.[7]

Evolution of US Cyber Command

The US Cyber Command was established in 2009 following an unprecedented cyber-attack on military computers attributed to Russia.[8,9] It was staffed through the Cyber National Mission Force, which was set up in 2012 and existed as a subordinate unified command under the US strategic command until it was raised to the status of a unified combatant command in 2018. Subsequently in 2022, the cyber mission force itself was raised to the status of a subordinate unified command under the Cyber Command.[10]

The Department of Defense (DoD)'s Cyber Strategy and the Command Vision for Cyberspace[11] published in 2018 stated, *inter alia,* that,

> …the Department seeks to pre-empt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause

---

7 Ibid., p.32.

8 William J. Lynn, "Defending a New Domain." *Foreign Affairs*, 30 May 2014 at www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain. Accessed on 13 January 2021

9 Brian Knowlton, "Military Computer Attack Confirmed." *The New York Times*, 25 August 2010 at www.nytimes.com/2010/08/26/technology/26cyber.html. Accessed on 18 September 2020

10 Unified Combatant Commands (UCCs) are organized either on a geographical basis, known as an "area of responsibility" (AOR), or on a functional basis, such as a special mission such as cyber. Subordinate Unified Commands are components of UCCs. A UCC is responsible for military operations within its geographic or functional area while its subordinate unified commands execute those operations and focus specifically on their assigned tasks and missions. B. Inamete, U. (2022, January 7) Ufot B. Inamete, The *Unified Combatant Command System Centerpiece of the 1986 U.S. Armed Forces Reforms*, Marine Corps University Press, 2022 athttps://www.usmcu.edu/Outreach/Marine-Corps-University-Press/Expeditions-with-MCUP-digital-journal/The-Unified-Combatant-Command-System/ (Accessed on 16 April 2022).

11 See Appendix 2.

> 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.[12]

This was a continuation of the DoD's traditional mandate to focus only 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 the testimony in 2017 where the then Assistant Secretary of Defense for Homeland Defense and Global Security, Kenneth Rapuano had stated, "[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"[13]. With considerable pushback from Congress, which called for the DoD to do more, a process was set in motion to update the relevant legislation and authorities to make the military a more relevant player in cybersecurity. The DoD's Cyber Strategy and the White House's 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 the Cyber

---

[12] "US, Department of Defense Cyber Strategy." Department of Defense, 2018 at media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF Accessed on 13 January 2021

[13] Mark Pomerleau, "DoD Says It Shouldn't Protect Homeland from Cyberthreats; McCain Disagrees." *Fifth Domain*, 13 September 2018 at www.fifthdomain.com/congress/capitol-hill/2017/10/19/dod-says-it-shouldnt-protect-homeland-from-cyberthreats-mccain-disagrees/ (Accessed on 14 January 2021).

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 the higher ups in the chain of command, as well as across agencies.[14] Whilst the earlier policy was designed to ensure that cyberspace operations of the military did not impact on 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 Islamic State of Iraq and Syria (ISIS). [15]

The Cyber Command's efforts to reinvent itself under the new mandate can be traced through successive speeches by the then Head, General Nakasone which are filled with buzzwords like defending forward and persistent engagement.[16] 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 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 the traditional domain to pinpoint attack and responses, did not lend

---

[14] Adam K Raymond, "Trump Makes It Easier for the Military to Launch Cyberattacks." *Intelligencer*, 16 August 2018 at nymag.com/intelligencer/2018/08/trump-makes-it-easier-for-the-u-s-to-launch-cyber-attacks.html (Accessed on 29 November 2020).

[15] Eric Geller and Jason Schwartz, "Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand," *Politico*, 16 August 2018 at www.politico.com/story/2018/08/16/trump-cybersecurity-cyberattack-hacking-military-742095 (Accessed on 19 October 2020).

[16] Paul Nakasone and Olivia Gazis, RSA Conference, 6 March 2019 at www.rsaconference.com/videos/strategic-competition-the-rise-of-persistent-presence-and-innovation (Accessed on 12 January 2021).

themselves well to the cyber domain.[17] Relevant provisions of the John McCain National Défense Authorization Act for fiscal 2019 gave the legislative authority to rewire the Cyber Command.

Cyber Conflict and Strategic Deterrence

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 US since the end of the Second World War.

The DoD's Cyber Strategy of 2015 highlighted the major requirements for credible deterrence in cyberspace. The key elements were response, common denial and resilience, and the end goal was to deter State and non-State actors from conducting cyber-attacks against US interests through "a range of policies and capabilities to affect a state or non-state actors' behavior".[18] A task force on cyber deterrence, which was set up in 2017, defined it as "the use of both deterrence by denial and deterrence by cost imposition to convince adversaries not to conduct cyber-attacks or costly cyber intrusions against the United States."[19]

That said, the concept of deterrence has proved to be difficult to adapt to cyber security. This was reflected in the testimony of the Director of National Intelligence James Clapper to the Senate Armed Services Committee in 2017 wherein he said: "Unlike nuclear weapons,

---

17 Brad D. Williams, "Meet the Scholar Challenging the Cyber Deterrence Paradigm," *Fifth Domain,* 23 July 2017 at www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/ (Accessed on 16 January 2021).

18 Department of Defense, *The Department of Defense Cyber Strategy*, Washington, DC, April 2015, p.10.

19 Defense Science Board, *Task Force on Cyber Deterrence,* Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, Washington DC, February 2017 at http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf (Accessed on 16 October 2020).

cyber capabilities are difficult to see and evaluate and are ephemeral. It is accordingly very hard to create the substance and psychology of deterrence in my view."[20] 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. [21]

Structure of Cyber Command

The Cyber Command was created out of the Cyber Mission Forces, set up in 2012. Each Cyber Mission Force was further subdivided into the 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 DOD information networks, and preparing cyber forces for combat. Cyber Support Teams were also to be in place to provide analytic and planning support to the National Mission and Combat Mission teams. At its full strength, reached by 2016, the Cyber Mission Forces numbered 133, comprising 6200 personnel with about 2300 being hired in 2013 itself.[22] Of these, approximately 3000 serve on the Cyber Protection Force, about 1000 were staffed within the National Mission Force, and about 2000 with the Combat Mission Force. As far as the personnel assigned to each team, the break was to be 60-person National Mission Teams, 40-person Cyber Protection

---

20) "Stenographic Transcript Before the Committee on Armed Services, United States Senate, Hearing to Receive Testimony on Foreign Cyber Threats to the United States," 115th Congress, Session 1, 5 January 2017, p. 5, at http://armed-services.senate.gov/imo/media/doc/17-01_01-05-17.pdf Accessed on 14 January 2021

21 Matthew Gault, "The American Military Sucks at Cybersecurity." *Motherboard Vice*, 15 January 2019 at motherboard.vice.com/en_us/article/7xy5ky/the-american-military-sucks-at-cybersecurity (Accessed on 13 October 2020).

22 Wyatt Olson, "Cyber Command Trying to Get Running Start, Add Staff." *Stars and Stripes*, 11 December 2014 at www.stripes.com/news/cyber-command-trying-to-get-running-start-add-staff-1.318612 (Accessed on 15 January 2021).

Teams and 60-person Combat Mission Teams.[23] The 13 national mission teams were to be supported by 8 national support teams, and the 27 combat mission teams with 17 combat support teams.[24] There were to be 18 national cyber protection teams (CPTs), 24 service cyber protection teams and 26 combatant command and DoD Information Network CPTs.[25]

The target date for full operational capability was extended to 2018 and reaching that milestone was announced on 17 May 2018.[26] The proportion of the Army and the Navy in the Cyber Command was at 60 per cent, with Air Force and Marines comprising the remaining 40 per cent. [27] Inductees attended training courses that ranged between 10-27 months. The total budget for setting up the US Cyber Command was $2 billion. [28]

---

[23] Aliya Sternstein,. "Need a Job? Cyber Command Is Halfway Full." *Nextgov*, 06 February 2015 at www.nextgov.com/cybersecurity/2015/02/need-job-cyber-command-halfway-full/104817/(Accessed on 16 October 2020).

[24] The most recent data available shows that the current teams consist of 13 National Mission Teams, 68 Cyber Protection Teams, 27 Combat Mission Teams and 25 Support Teams. A further breakup of the operational teams indicates that the Army supplies 41 teams, the AFCYBER supplies 39 teams, the navy supplies 40 teams and the Marines provides 13 teams.

[25] Mark Pomerleau, "Here's How DoD Organizes Its Cyber Warriors." *Fifth Domain*, 25 July 2017 at www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/ (Accessed on 18 September 2020).

[26] Mark Pomerleau, "Cyber Command Reaches Critical Staffing Milestone." *Fifth Domain*, 18 May 2018 at www.fifthdomain.com/dod/cybercom/2018/05/17/cyber-commands-cyber-warriors-hit-key-milestone/ (Accessed on 15 January 2021).

[27] Joseph Marks, "US Army, Navy Cyber Commands Ready Far Ahead of Schedule," *Defense One*, 3 November 2017 at www.defenseone.com/threats/2017/11/us-army-navy-cyber-commands-ready-far-ahead-schedule/142287/ (Accessed on 21 January 2021).

[28] Aliya Sternstein, "US Military Cybersecurity by the Numbers", *Nextgov*, 22 December 2016 at www.nextgov.com/cybersecurity/2015/03/us-military-cybersecurity-numbers/107637/(Accessed on 16 January 2021).

Retaining human resources has proved to be one of the biggest problems for the Cyber Command, so much so that applicants are given a service incentive to remain and to combat the notion that it would lead to career stagnation.[29] The Army for instance, offered a service retention bonus of $7,900 to $50,400 depending on expertise and experience. [30] 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".[31] The composition of civilians in Cyber Mission Forces was in the range of 20 per cent in 2016. [32]

A Cyber Accepted Service was established by Congress in 2016 to deal with this issue. The main purpose was to provide agility and flexibility for the recruitment, retention, and development of high-quality cyber professionals within the Department of Defense. It also provided for an accelerated civilian hiring process.[33]

Other State Actors

Other State actors have only recently been coming to prominence since the US government has historically played a minor role in the

---

29 "Army Braces for a Culture Clash." *Signal Magazine*, 4 January 2016 at www.afcea.org/content/Article-army-braces-culture-clash (Accessed on 18 August 2021).

30 David Ruderman, "Army Offers Selective Retention Bonuses to Retain Enlisted Cyber Warriors." *www.army.mil*, 29 May 2015 at www.army.mil/article/149561/army_offers_selective_retention_bonuses_to_retain_enlisted_cyber_warriors (Accessed on 12 August 2021).

31 "Cyber Chief: Army Cyber Force Growing 'Exponentially'." *www.army.mil*, 5 March 2015 at www.army.mil/article/143948/cyber_chief_army_cyber_force_growing_exponentially (Accessed on 8 October 2020).

32 "Event Coverage of 2015 AUSA Annual Meeting & Exposition." *The CyberWire*, 12 October 2015 at thecyberwire.com/events/ausa-annual-meeting-and-exposition-2015.html. (Accessed on 16 August 2020).

33 James Di. Paine, "Cyber Warfare and U.S. Cyber Command." The Heritage Foundation, 24 January 2024 at www.heritage.org/military-strength/assessment-us-military-power/cyber-warfare-and-us-cyber-command. (Accessed on 28 January 2024).

development of cyberspace. Other than the initial impetus provided by the government to create a network that could withstand a nuclear explosion, much of the technical development was carried out in universities and other specialized agencies. Subsequently, the private sector had provided the impetus, a fallout of that being that not much attention was paid to the security side of the domain.

National Security Agency

The National Security Agency was established in 1952 although its existence was officially revealed only in 1975. Its main objective has been signals intelligence, though the advent of computing has seen it increasingly shifting to mass data collection and computer espionage. It lists its core missions and functions as below :

1. Provide intelligence to warn of malicious cyber threats and information US Government (USG) policy;

2. Develop integrated Nuclear Command & Control Systems threat, vulnerability, risk, and cryptographic products & services;

3. Release integrated threat, assessment, and mitigation/protection products for the DoD and USG customers;

4. Execute high-assurance cryptography and security engineering;

5. Offer combined defence/offence operations with key government partners;

6. Enable the defence of the agency's networks in coordination with NSA's Chief Information Officer;

7. Promote information sharing to support the agency's cybersecurity mission.[34]

The Snowden revelations of 2013 brought out the extent to which the NSA intercepted and stored communications and metadata. It is

---

[34] US, NSA Cybersecurity: Core missions. National Security Agency at https://www.nsa.gov/Cybersecurity/Overview/ (Accessed on 27 January 2024).

estimated to have an employee strength of over 32,000 and the budget in excess of $10 billion.

Department of Homeland Security

The Department of Homeland Security, created after the 9/11 attacks, is responsible for domestic defence. Its national cyber security division is responsible for critical infrastructure. It houses a number of entities including Cybersecurity Infrastructure Security Agency (CISA), the leading civilian cybersecurity agency. CISA works with government and private sector organisations to enhance the security and resilience of critical infrastructure sectors, such as energy, transportation, communication, and healthcare.[35] It also operates the national cyber response coordination group, which comprises 13 federal agencies and is responsible for coordinating the federal response in the event of a nationally significant cyber incident.

The National Cybersecurity and Communications Integration Center (NCCIC)

The NCCIC is a 24x7 cyber situational awareness, incident response, and management center that coordinates various aspects of the US federal government's cybersecurity and cyberattack mitigation efforts through cooperation with civilian agencies and the private sector.[36] It performs various tasks which include sharing actionable intelligence, assessing risks, and providing situational awareness to stakeholders.

Cyber Threat Intelligence Center

The Cyber Threat Intelligence Center was set up as a coordinating agency in 2015 within the office of the Director of National Intelligence.

---

[35] Cybersecurity and Infrastructure Security Agency CISA, *Cybersecurity Best Practices* at https://www.cisa.gov/topics/cybersecurity-best-practices (Accessed on 28 January 2024).

[36] CISA, "NCCIC ICS Fact Sheet" at https://www.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_NCCIC%20ICS_S508C.pdf (Accessed on 27 January 2024).

Its mission is to provide integrated all-source analysis of intelligence related to foreign cyber threats or incidents affecting US national interests. Its primary functions include serving as a central hub for collecting, analysing, and integrating cyber threat intelligence from various agencies and sources. It focuses on identifying and understanding emerging cyber threats, their potential impact on national security, and the techniques used by threat actors. It also works closely with other government agencies, including the intelligence community, law enforcement, and cybersecurity organisations, to coordinate the sharing and analysis of cyber threat intelligence. As an intelligence collection centre, it tries to improve collaboration to improve the government's collective understanding of cyber threats and enable a unified response to imminent threats. It is perceived as playing a crucial role in strengthening the US government's situational awareness and response capabilities in the face of cyber threats.[37]

The Central Intelligence Agency

The Central Intelligence Agency also has a cyber division operating under the rubric of the Information Operations Center. Historically, the rivalry has been between the CIA and the NSA once consensus broke down that the NSA would stick to exfiltration data in transit while the CIA would carry out the physical leg work of espionage. However, when the NSA gained the capability to hack into computers and gather information, the CIA endeavoured to regain its position by establishing a new office called the Clandestine Information Technology Office (CITO) in 1995. This office later evolved into the Information Operations Center (IOC).

To briefly sum up, the United States demonstrated early recognition of the strategic implications of the cyber domain and developed doctrines concerning information warfare. However, adapting existing doctrines to effectively engage in cyberspace warfare has presented

---

[37] Office of the Director of National Intelligence, "The Cyber Threat Intelligence Integration Center" at https://www.dni.gov/index.php/ctiic-home (Accessed on 27 January 2024).

challenges. The cyber environment is highly complex and multidimensional, making it difficult to achieve objectives compared to traditional domains. Despite declaring cyberspace as the fifth domain of warfare, it has been difficult to fully integrate it as a major theatre of conflict. The rapid evolution of the cyber domain has led to fragmented responsibilities among different organisations, particularly in intelligence and cyber exploitation. Policy makers have struggled to assign a dominant role, as seen in the case of the National Security Agency and Cyber Command. Efforts to separate the two have not been successful, highlighting the ongoing challenges in managing and adapting to the cyber domain.

Chapter 3

Russia: Agencies in a Perpetual Tug-of-War

Underpinnings of Russia's Cyber posture and strategy

Like most countries studied for this monograph, the Russian approach towards cyber warfare is largely conditioned around historical factors and existing approaches and strategies, with many of them developed over decades of waging an information war. The Russians, in fact, club cyber war and information war together, believing them to be two sides of the same coin. In this regard, there are a lot of similarities between the Russian and Chinese approaches in that both see information war as a constant low-intensity conflict.[38]

In recent times, what has triggered Russian interest in this arena, and its use for military purposes was the use of information technology in the 1991 Gulf War based on the Revolution in Military Affairs (RMA).[39] Russian military theorists also began to conceptualise information warfare as comprising the entire gamut of computer network operations, electronic warfare, psychological operations, and information operations.[40] Such an articulation 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

---

[38] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare", Center for Naval Analyses, 2016, p.i.

[39] B. Lilly and J. Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces", 12th International Conference on Cyber Conflict (CyCon), 2020, p.8.

[40] Michael Connell and Sarah Vogler, no.38, p.2.

Sciences in February 2013, followed by an article in a military journal. In the article, the points of relevance he made were as follows:

> "The experience of military conflicts, including those related to the so-called color revolutions in North Africa and the Middle East, confirms that a completely prosperous state in a matter of months and even days can turn into an arena of fierce armed struggle, become a victim of foreign intervention, plunge into the abyss of chaos, humanitarian catastrophe and civil war.… Information confrontation opens up wide asymmetric opportunities to reduce the enemy's combat potential. In North Africa, we have witnessed the implementation of technologies to influence government structures and the population through information networks."[41]

Thus, unlike Western conceptualisations which segregated the various aspects of cyber and tried to apply existing rules of the road to this new domain, the Russian approach "in keeping with traditional Soviet notions of battling constant threats from abroad and within", has been to perceive "the struggle within "information space" to be more or less constant and unending."[42] The internet, and the free flow of information it engenders, is viewed as both a threat and an opportunity in this regard in that, while the domestic arena must be protected against all such attempts at disinformation and destabilization, it provides Russia with the chance to do the same to hostile powers.[43] To this end, Russia has been an active player in cyberspace, realising early on that it could be used to serve its national interests particularly when it came to moulding the neighbourhood which had been volatile ever since the breakup of the Soviet Union. The first inkling of this came during the war with Georgia in 2008 in which information and influence operations played a big part. However, most of those activities were done by the intelligence agencies, with the military sticking to its traditional role as a

---

41 Valery Gerasimov, "The Value of Science Is in the Foresight", (translated from the original Russian*), Military Review*, January-February 2016, pp.23-29.

42 Michael Connell and Sarah Vogler, no. 38, p.i.

43 Ibid., p.i.

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 its 'cyber troops'. [44] 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 related strategy documents 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*.

Conceptualisations of cyberspace

Many analysts have started their analysis with the US mischaracterisation of Russian activities in cyberspace based on its own perceptions of the domain. Some go so far as to say that Russia has a better conceptualization of cyber warfare as a grand strategy as opposed to thinking about it purely in tactical terms.[45] According to the same analysts, the US has a tendency to "mirror image when analyzing our adversaries in cyberspace, to an even greater degree than in other warfare domains. We make uninformed assumptions about their motivations, intentions, and risk calculus based on U.S. thinking and conceptualizations of cyber."[46]

Therefore, a better understanding of Russian activities in cyberspace maybe gained by looking at the entire gamut of Russian activities in cyberspace through a Russian lens. In the first instance, according to Janne Hakala and Jazlyn Melnychuk, information confrontation is a more appropriate term to use than information warfare since this

---

[44] N. Popescu and Secrieru S. Hacks, "Leaks and Disruptions: Russian Cyber Strategies", Chaillot Paper, 149 at https://www.iss.europa.eu/content/hacks-leaks-and-disruptions-russian-cyber-strategies, p.18 (Accessed on 19 February 2022).

[45] Michael Connell and Sarah Vogler, no.38, p. 2.

[46] Ibid, p.2.

highlights it 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 adversary's information infrastructure while protecting its own objects from similar influence".[47] Like China, the Russians also seem to have amalgamated kinetic operations with non-military and psychological operations. Studies also show that there is a continuing discussion as to whether non-military measures should be placed higher than military measures in the current context. Similar debates have been raging in the West, but they have largely been stymied by the military industrial complex which would run the risk of losing enormous funding if such a conceptualisation were to take place.

Russia has been coming out with information doctrines since 2000 and succeeding doctrines 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."[48]

Russia's Ministry of Defence's *Concept on the Activities of the Armed Forces of the Russian Federation in the Information Space* (2011) provided a clear definition of information warfare as "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 destabilize the state and society, as well as coercing the state to take decisions for the benefit of the opposing force."[49]

---

47 Quoted in Janne Hakala, Jazlyn Melnychuk, "Russia's strategy in cyberspace", *NATO Cooperative Cyber Defence COE*, June 2021, p.5.

48 Quoted in B. Lilly and J. Cheravitch, no. 39, p.6.

49 Ministry of Defence, Russian Federation Armed Forces' Information Space Activities Concept' at https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle, 2011 (Accessed on 13 June 2021).

This definition makes it clear that the Russians combined both the pipes through which the data flows, as well as the data itself as being a critical part of information warfare. By extension, therefore, Russian forces also had to be prepared for similar actions from their opponents. Like the Chinese, the Russians also believed that information warfare and cyber operations are continuous and can be undertaken before any official declaration of war and are a legitimate tool to achieve political objectives without undertaking kinetic operations. That said, the basic thrust of these doctrines has been to push the line that Russia is at the receiving end of continuous attacks meant to destabilise it. The 2016 doctrine emphasized increasing threats emanating from the information cognitive space, primarily driven by foreign actors, and their effects on social values and stability, but adopted a defensive and cooperative posture.[50] Policies enunciated have included legislation to regulate entities that are engaged with the information sphere and enhancement of the "security of critical information infrastructure." International policy recommendations range from the "formation of a system of international information security" to "the formation of mechanisms for international cooperation in countering the threats of the use of information and communication technologies for terrorist purposes."[51]

Even in instances where the role of the military has been conceptualised such as in the document *Conceptual Views on the Activities of the Armed Forces in the Information Space* (Ministry of Defence, 2011), where the vulnerability has been characterised as the widespread use of computer technology in command and control systems of troops and weapons, the proposed policy response has been to work "on the basis of a set of principles: legality, cooperation with friendly states and international organisations; and containment and prevention of military conflicts in the information space."[52] This thread has continued in succeeding

---

[50] B. Lilly and J. Cheravitch, no. 39, p.7.

[51] Ibid. p.7.

[52] An unofficial translation of this document can be found at https://ccdcoe.org/uploads/2018/10/Russian_Federation_unofficial_translation.pdf (Accessed on 15 July 2021).

documents even as the threats outlined have gathered apace. It is only the most recent document titled, *Doctrine of Information Security of the Russian Federation* published in 2016, that 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 neutralization of information psychological impact, including aimed at undermining the historical foundations and patriotic traditions associated with the defense of the Fatherland."[53]

This dichotomy between what the Russian State says and what it does is one of convenience. Even though Russia does not officially have an offensive cyber policy, it has been actively engaged in thinking about offensive weapons and there is a large amount of literature that reflects Russian thinking on cyber weapons. Cyber weapons can be used to conduct hostile operations from any location and can weaken the enemies' ability to defend themselves and retaliate. There is no need to cross borders or have a physical presence in the enemies' territory. Most importantly, offensive cyber capabilities can be considered as asymmetric actions that can help a technological and economically weaker State, which Russia considers itself to be and therefore, by extension, Russia is well within its rights to undertake such actions. Lastly, offensive actions mean taking the initiative rather than emphasising a defensive posture which might or might not succeed. Another important aspect is that even though signalling to the top leadership may not be possible through cyber actions, they can have a huge psychological effect on the general population especially if the infrastructure is targeted. It is a different issue that information infrastructure can relatively swiftly come back online as opposed to physical destruction of the same infrastructure. In most cases, with critical infrastructure, the vulnerabilities already exist and only have to be located in order to compromise the system, either for collecting

[53] A translation of this document can be found at https://publicintelligence.net/ru-information-security-2016/ (Accessed on 14 October 2020).

information or for disrupting it. Even if cost calculations are taken into account, the amount required to create such weapons, which is largely a function of the manpower needed, is much cheaper than estimates of other countries such as the United States because manpower is much cheaper in Russia.[54] "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 – a classic justification for a number of Russian policies, including investments in military modernization."[55]

Main State actors

There are two schools of thought on the structure of State agencies dealing with cyberspace in Russia. There are those who say that it is highly centralised and others who say that it is more decentralised today than before with the government giving a broad framework of goals to be achieved and leaving the agencies to achieve those goals without going into the details. The latter framework has the danger of leading to escalation since the agents on the ground are not at liberty to understand the geopolitical implications of their actions. According to Hakala, the latter has become the reality because Russian intelligence agencies engage in competitive intelligence, trying to engage in hacks which they believed to be useful to the leadership, the successful completion of which would give them access to more resources and influence.[56] Each tried to prove to the Kremlin that it is more useful to secure greater access to the Kremlin's levers of power and patronage, but also increased funding and privileges.[57]

---

54 B. Lilly and J. Cheravitch, no. 39, p.10

55 Ibid. p.11.

56 Janne Hakala, Jazlyn Melnychuk, no. 47, p.17.

57 N. Popescu and Secrieru S. Hacks, no. 44, p.30. Detailed analyses of each of these organisations can be found in the following article: Soldatov, Andrei, and Irina Borogan. "Russia's surveillance state," *World Policy Journal,* 30 (3), 2013, pp. 23-30. A more detailed analyses on the FSB can be found in Ulf Walther, "Russia's Failed Transformation: The Power of the KGB/FSB from Gorbachev to Putin", *International Journal of Intelligence and CounterIntelligence*, 27 (4), 2014, pp. 666-686.

Among the various State agencies operating in this field, the largest is the Federal Security Service (FSB), which is widely regarded as the successor to the KGB. The FSB's influence extends beyond national borders due to the borderless nature of the Internet. This agency possesses specific legal authority to monitor and intercept Russian data traffic, granting it certain advantages. The activities undertaken by the FSB are considered highly sophisticated and are perceived to hold long-term significance.

The Glavnoye Razvedyvatelnoye Upravlenie (GRU), or the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, serves as the military's external intelligence agency. In terms of its actions, the GRU appears to exhibit a more aggressive and visible approach, with a focus on offensive cyber operations. It consists of two primary units, namely the 85th Special Service Unit and the Main Centre for Special Technologies, both of which have a notable track record of operations. Additionally, there is a third unit called the 72nd Special Service Centre, which specializes in the use of proxies and front organisations. These units are often recognized through the Advanced Persistent Threat (APT) groups that operate under or in coordination with them.[58] The SVR, or the Foreign Intelligence Service, is another external intelligence agency, alongside the GRU. However, the SVR appears to have a distinct focus primarily on espionage operations, differing from the other agencies that engage in sabotage and information operations as well.

Of the organisations listed above, the FSB and the GRU undertake the lion's share of activities in cyberspace. 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. Consequently, it had developed relations with Russian hackers from

---

[58] B. Lilly and J. Cheravitch, no.39, p.17-19. This facet is also picked up by Josephine Wolff in her Paper for the Foreign Policy Research Institute. Josephine Wolff. "Understanding Russia's Cyber Strategy", FPRI, 2021 at https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/ (Accessed on 22 February 2022).

the early 1990s. Russia's wars with Georgia and Estonia also saw the FSB largely playing a leading role since these countries had been part of the former Soviet Union and the FSB had existing intelligence apparatus in these two countries. So, 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 direct support of the military."[59]

A number of reasons have been given for the re-establishment of the GRU's position as a purveyor of cyber operations. One reason was that alliances like NATO also began to coordinate among member countries on cyber as well as growing US capabilities and intention to shift more responsibility of cyber operations to the military. This was manifest through the establishment of their cyber command in 2009.

The GRU began to receive attention and resources from 2013 as part of the Russian Defence Ministry's attempts to improve and advance the militaries' research and development on cyber operations, signals intelligence and electronic warfare. 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. Other indications of re-emphasis on the domain were research by the military research and development organisations, including increased recruitment at the FSB's Cryptography Institute, and increasing dissertations related to computer networks and articles related to cyber capabilities in Russian information warfare journals.[60] The increasing sophistication was also reflected in operations such as the attack on the Ukrainian energy grid which saw remarkable change between 2015 and 2016.

While the FSB got the bulk of organisations research that predated Russia, the GRU has added new aspects of information warfare such as DDoS attacks into the curricula of Russia military universities. There are a number of specialized units within the GRU, including the 72nd

---

59 Janne Hakala, Jazlyn Melnychuk, no. 47, p.11.

60 Ibid. p.12.

Special Service Centre (Unit 54777), and the 85th Special Service Centre. During the Ukraine crisis, it was also seen that specialists worked with local commands to conduct operations.

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."[61]

They conclude their analysis by saying that although currently, offensive cyber warfare is not formalised in Russia's military doctrines, this could go in two directions. Military planners might feel the need to write up new doctrines in order to integrate cyber within the existing military

---

[61] Ibid. p.20.

frameworks, or the policy makers might feel the current posture of plausible deniability would be better served by keeping its cyber policies as opaque as possible. Russia's own actions are therefore perceived by it as being completely defensive in nature aimed at preventing potential conflicts and controlling conflict escalation by remaining below the threshold of armed conflict.[62]

Russia is taking advantage of what it perceives as Western confusion on the subject; the insistence on cyber security looking at only the security of the networks and not the content, making a clear distinction between war and peace without considering the grey zones and the so-called grey zone warfare. It therefore undertakes activities below this threshold, thus allowing it to retain the upper hand to remain unpredictable and achieve its objectives without entering into conflict. The Western fascination with maintaining an open, free and stable internet is also taken advantage of. As far as the Russians are concerned, those three words are an oxymoron and in fact, they make Western countries more vulnerable and open to exploitation and attacks. On the flip side, the Russian obsession is with ensuring that its cyberspace is secure and not available for retaliatory attacks. Russia's perception has largely been governed by its experience particularly in the post-Soviet period when it perceived Western countries seeking to inflict further dissension through the so-called Colour Revolutions and the social media-generated protests in Russia at various points in time. This perception can be seen in the *Information Security Doctrine* (2016), which states that, "intelligence services of certain states are increasingly using information and psychological tools with a view of destabilising the internal political and social situation in various regions across the world, undermining sovereignty and violating the territorial integrity of other states. Religious, ethnic, human right organisations as well as separate groups of people, are involved in these activities and information technologies are extensively used towards this end."[63]

---

62 Ibid., p.9.

63 See no. 53.

Cyber conflict and strategic deterrence

The cyber arsenal is considered part of the strategic arsenal given that nuclear weapons and conventional weapons alone are not sufficient to deal with the entire spectrum of threats confronting a State today. The overall goal is to achieve strategic effects and gain superiority over the opponent without inviting retaliatory action to the extent possible.[64] This may be a key reason why cyber-attacks aimed at physically impacting infrastructure are wielded more sparingly as they may trigger a more dramatic response making escalation harder to control. To what extent escalation can be controlled is a big question considering that cyber is very attractive as a substitute for conventional force, especially in attacking critical infrastructure such as energy transport and banking but the US and UK have warned that cyber-attacks may be responded to with conventional force. The strategic effect is seen to be achieved by making the population uncertain about the reliability of the information infrastructure that they are using.

Russian officials, academics, and military personnel have largely been dubious about the notion of cyber deterrence in the context of attributing cyber-attacks accurately. As noted by influential figures such as Gerasimov, Krutskikh, Ivanov, and Yashchenko, this lack of attribution capability makes any form of cyber deterrence ineffective and challenging to pursue. [65]

Securing the information space

So, what are the foundational beliefs for Russia in cyberspace? Russia views control over its domestic information space as essential to its security and has pushed the idea of digital sovereignty. In October 2019, a law was passed which aimed to have only 10 per cent of

---

[64] Ibid., p.12.

[65] J. Meakins, "Russia's Approach to Cyber Deterrence", European Leadership Network, 2021, p.7 at https://www.europeanleadershipnetwork.org/wp-content/uploads/2018/07/Living-in-Digital-Denial-Russia%E2%80%99s-Approach-to-Cyber-Deterrence.pdf Accessed on 21 December 2021

Russian Internet traffic routed through foreign servers by 2024. However, the practical implications and the complete extent of these implementations remain to be assessed in the months leading toward the 2024 target. The Russian Internet is now quite large consisting of search engines and social media sites including Yandex and VKontakte. This has also enabled Russia to reach out to Russian-speaking minorities in neighbouring countries thereby extending Russia's sphere of influence in these countries through the digital space. There is also increasing censorship in the Russian Internet. On the flip side, it also reduces Russia's influence abroad since people abroad will be unable to browse through the Russian Internet.

As far as the military aspect is concerned, the system would create a deterrence by denial effect that would deny the adversary the ability to take hostile action in this closed and closely monitored Russian Internet space. Russia would also be able to conduct attacks on the open Internet networks of other States they would not be able to do so in the closed network of Russia.

Several other benefits seen to accrue from this measure including the development of Russian hardware and software, the ability to access data and content, and to protect the data from foreign exploitation, secondly, the ability to remove and restrict websites that are considered to be anti-national, better ability to target anti national activities through counter intelligence, law enforcement and censorship, protecting critical information infrastructure by bringing it under State ownership.[66]

Controls over Russian Internet

"Information-technological and information-psychological counter-measures[are] managed by State-controlled or affiliated news services and educational, patriotic and religious institutions, as well as through the cyber capability of security services and the military. It controls a domestic information environment and conducts covert espionage and influence and cyber operations abroad to prevent possible threats from

[66] Janna Hakala quoted in Janne Hakala, Jazlyn Melnychuk, no. 47, p.13.

emerging."[67] There are also existing systems in place from the Soviet era for surveillance as well as new systems being developed.

A 2012 policy defined critical information infrastructure and introduced the national cyber security system which is "designed to shield all government information resources within single system with a constantly monitored perimeter. This shield would extend to all resources and critical infrastructure so they all share information about cyber-attacks with the central office which would determine how an attack was mounted and distribute security recommendations to the rest of the system."[68] A 2017 law on critical infrastructure specified that the FSB would be in charge of the system. A large number of other laws have also been drawn up to assert complete control over the Russian Internet.

The role of the military

As seen above, the role of the military has been confined to the military intelligence agencies, and that too, in an opaque manner. The fusion of various subsets of military dealing with different aspects of the electromagnetic spectrum is yet to take place. However, there may be a method to this madness. Until recently, the armed forces were limited to electronic warfare. However, there have been reports about the establishment of cyber units within the military which also includes a wide variety of specialists including programmers, mathematicians, cryptographers and electronic warfare and communications experts. Russia depends more on the intelligence agencies and patriotic hackers and cyber criminals compared to the military. "Cyber criminals are preferred because they provide possible deniability, and they are cost effective with patriotic hackers often working for free."[69]

Russia is unique in combining cyber-attacks with psychological operations. Given Russia's active operations in cyberspace, there are many instances where this can be seen, the most prominent example

---

67 Ibid., p.13.

68 Ibid., p.15.

69 Ibid., p.15.

being Ukraine which has been characterised as a showcase of Russian means and methods. In this regard, Ukraine has also been a way for Russia to signal cyber capabilities as well as to provide a testbed for its cyber capabilities. Much before the attacks on the US electoral system, similar attacks were carried out on the Ukrainian presidential election in May 2014.

In summary, the approach to cyber warfare by various countries, including Russia, is shaped by historical factors and existing strategies developed through years of waging information war. Both Russia and China view information war as a constant low-intensity conflict, considering cyber war and information war as interconnected. Russia's interest in cyberspace and its military use was triggered by the use of information technology in the 1991 Gulf War and the concept of information warfare encompassing computer network operations, electronic warfare, psychological operations, and information operations.

Ukraine has served as both a testing ground and a signalling platform for Russian cyber capabilities, with attacks on the Ukrainian presidential election preceding those on the US electoral system. This pattern continues with the continuing conflict in Ukraine and there are already evident signs of re-organisation of Russian cyber tactics and strategies drawing on the lessons learnt for the cyber and cyber-enabled aspects of the conflict.

While the Russian military in general has operated on the sidelines when it comes to cyberconflict, there would be plenty of lessons drawn from the Ukraine conflict that could lead to better integration of cyber into existing doctrines.

Chapter 4

China: Root and Branch Overhaul

Underpinnings of Chinese cybersecurity

To understand the Chinese perspective of cyber security, one has to begin with certain foundational precepts which have guided Chinese domestic and security policy. The first of these is to do with informationisation, which was initially seen as crucial to economic progress but subsequently seen as the fulcrum on the basis of which all of China could advance. Informationisation was seen as a comprehensive system of systems, where "the broad use of information technology is the guide, where information resources are the core, where information networks are the foundation, where information industry is the support, where information talent is a key factor, where laws, policies, and standards are the safeguard".[70]

By the 1990s, there was an effort to refocus from building an information economy to an Information Society. In 2002, informationisation was formally recognised as essential for growing Chinese comprehensive national power. Creating an Information Society was seen as a way of leapfrogging the advanced economies which had come up largely during the second industrial age. While China could play catch up with the industrialised world by using its resources, its ambition was to go beyond the advanced economies by seizing on the latest information technologies.

---

[70] State Council Information Office, "Tenth Five Year Plan for National Economic and Social Development, Informationization Key Point Special Plan", quoted in Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, ABC-CLIO, 2016, p.1.

This policy extended to the military as well. China is an early adopter of cyber technologies in the military. It has been adapting technologies in general to make up for perceived deficiencies in weaponry and has found it all the more imperative to incorporate cyber and emerging technologies as a means of giving it an asymmetric advantage on the battlefield. It has had two objectives in this regard: to incorporate cyber into the military to increase its efficiencies as well as to use cyber as a domain to carry out attacks and gain advantage over the enemy.

The Chinese military also saw information technologies as crucial to fighting and winning future wars. To this end, the political and military leadership was willing to go to the extent of completely dismantling the existing structures and systems in order to build up a military that had information technology at its core. This necessitated not just revamping administrative structures but also strategic and operational principles.

However, the most revolutionary of the actions taken in order to bring information systems to the fore has been that of reorienting the military to conduct joint operations. It is almost a case of the tail wagging the dog in that in order to bring information systems into the military, it has been deemed necessary to destroy the existing structure and restructure it for joint operations. This was seen as such a crucial necessity that Joint Operations found their way into the eighth and ninth Five-Year Plans, thus making them "a matter of national interest."[71]

The trigger for incorporating technology into the military has largely been traced to the Gulf War of 1991. The military strategy guidelines of the Central Military Commission of the Chinese Communist party brought out in 1993 directed the PLA to "place the basis of preparations for military struggle on winning local wars that might occur under modern especially high technology conditions." Chinese military and academic researchers have continuously sought to overcome the tendency to think of ways to fight the last war and concentrated on the next generation of warfare while ignoring the current situation and

---

[71] Ibid., p.27.

requirements. There have been voices that have cautioned against this tendency within Chinese academia, especially the urge to look on technology as a panacea and an end in itself rather than a means to an end.

In this sense, cyber is a small but important cog in the overall scheme of things, since it forms the core of the system-of-systems around which infomationised warfare functions. Where other militaries are conceptualising the role of the military in cyberwarfare, Chinese military planners are trying to conceptualise how to extend the boundaries of cyber warfare and information warfare.

Conceptualisations of cyber warfare

In terms of conceptualisation, the consensus is that the Chinese have made major strides in expanding the horizons of cyber warfare. On the strategic side, for the Chinese, informationised warfare extends beyond cyber activities and is instead about establishing information dominance. This involves being able to gather, transmit, analyze, assess, and exploit information more quickly and more accurately than one's adversary. "Winning future wars will depend upon winning information dominance, while denying it to the adversary."[72] Information warfare comprises an extensive array of information operations. These include reconnaissance operations, offensive and defensive operations, and deterrence operations, in the electromagnetic, network, and psychological realms. It also includes the employment of physically destructive means against key information infrastructure targets, ranging from satellite constellations to landlines and command posts. Just as information warfare is about more than computer network warfare, information operations involve more than just interfering with information systems.[73]

The *Science of Military Strategy* (2001) document focused on hi-tech local war. Among the observations it made were that wars had become

---

[72] Dean Cheng,no. 70, p.16.

[73] ibid

localised with more emphasis on destroying the information infrastructure, both military and civilian. It found merit in Mao Zedong's principle "you fight in your way and we shall fight in ours" as meaning that principles and doctrines should not be borrowed from others or based on reaction to an adversary's doctrine.

All of these were brought together in the 2013 edition of the *Science of Military Strategy*, and following its publication, large-scale reforms were initiated including the establishment of the strategic support force. This was accompanied by discussions on the role of cyber warfare in the larger strategic environment. It was at this time that the US Department of Defense released its *Defense Cyber Strategy* with its emphasis on cyber deterrence. Chinese analysts went to great lengths to criticise the US document for destabilising cyberspace through its emphasis on offensive and defensive cyber operations as part of a two-pronged deterrent strategy of deterrence by denial and deterrence by punishment. To counter this, Chinese strategists enunciated a policy of active defence, which also requires the build-up of cyber forces.

Mao first propounded Active Defence in 1936, which he described as "defence for the purpose of counter-attacking, and taking the offensive."[74] The concept of active defence was subsequently incorporated into military strategy. The essence of active defence is that China adopts a strategically defensive posture, in which China will not "fire the first shot" but will use offensive actions to achieve defensive goals. Other important elements of active defence include seeking to deter war, if possible, and mobilizing national support under the idea of "People's War".[75] The emphasis was on retaking the initiative and

---

[74] Rosita Dellios, *Chinese Strategic Culture: Part 1 - The Heritage from the Past*, Centre for East-West Cultural and Economic Studies, No. 1, Bond University,1994 at https://pure.bond.edu.au/ws/portalfiles/portal/28738438/Chinese_strategic_culture_Part_1.pdf (Accessed on 15 October 2020).

[75] M. Taylor Fravel, "China's Changing Approach to Military Strategy: The Science of Military Strategy from 2001 and 2013", in Joe McReynolds (ed.), *The Evolution of China's Military Strategy*, Jamestown Foundation, Washington DC, 2016, p.6.

information technology was seen to be the means though which the initiative can be seized. It also meant using the enemy's dependence on information technology against it by disrupting their communications, command and control and logistics networks.

This was to be achieved through integrated electronic and network warfare. Whilst electronic warfare referred to the degradation and disruption of the enemy's electronic systems, network warfare is the other side of the coin of electronic warfare. "It covers the range of activities that occur within networked information space, as the two sides attack each other's networks while preserving their own. Like electronic warfare, it includes not only offensive and defensive components but also reconnaissance of the adversary and others' networks."[76] This was apace with joint operations which itself had become a touchstone for the Chinese military.

Much study went into joint operations before the momentous reforms of 2015. The existing military structure consisted of services and branches and the existing concept of joint operations were those operations that involved two or more services while combined operations were those that that involve two or more branches of the same service.[77] However, these were *ad hoc* creations and did not benefit from the advances in information technology, which would lead to flexibility in operations and real-time responses. That required common situational awareness. PLA descriptions of the nature of future war also reflected changing perceptions within the military. If in the 1990s, the formulation was that of preparing for local wars under modern local high technology conditions, later formulations talked about local wars under informationised conditions.

Other documents that have unveiled Chinese thinking on the role of the military in cyber defence are the White Papers on China's military strategy that come out periodically. The first White Paper to have an in-depth analysis of the relevance of information warfare came out in

---

[76] Dean Cheng, no. 72, p.99.

[77] Ibid., p.27.

2004. Noting the transition of the role of the military over the last two decades, and the way in which it fought wars as exemplified by the Gulf Wars, the White Paper called for an equivalent revolution in military affairs as had been undertaken by the US military with considerable success. Information in real time from the battlefield to the commanders as well as command automation were the major takeaways from these examples. The 2010 White Paper went into detail on the cyber aspect, noting that States are working towards enhancing their capabilities to carry out cyber operations and worked out strategies for cyberspace. The 2014 White Paper called for the development of a cyber force to be prepared for any cyber contingencies. It also called for the establishment of integrated combat forces that would focus on system versus system operations featuring information dominance, precision strikes and joint operations. The focus on information warfare was largely pushed by Xi Jinping who had become General Secretary of the Chinese Communist Party and Chairman of the Central Military Commission in 2012, and President of China in 2013. In widely reported remarks to the Politburo in 2014, he called for refocusing the PLA towards information warfare saying, "Faced with the severe challenges to our national security and stability and the deep-seated contradictions and problems with reform, it is even more pressing that we greatly liberate our ideas and concepts, have the courage to change our fixed mindsets of mechanized warfare and establish the ideological concept of information warfare." He instructed the PLA to create a strategy for information warfare by establishing "new military doctrines, institutions, equipment systems, and tactics."[78]

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

---

[78] "Army Needs 'Information Warfare' Plan, Declares Xi", *China Daily*, 01 September 2014 at http://www.chinadaily.com.cn/china/2014-09/01/content_18520930.htm. (Accessed on 16 October 2020).

> 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 cyber force, and enhance its capabilities of cyberspace situation awareness…[79]

The 2019 White Paper on *China's National Defence in the New Era,* called for further development of the cyber capabilities of the military consistent with China's position as a major international power. The White Paper positioned China as a peer competitor to the United States and chose the US defence expenditure on cyber as its benchmark. The White Paper went beyond cyber capabilities and called for investment in cutting-edge technologies such as AI, quantum, big data, and cloud computing, to derive benefits for the military. These technologies could be used to develop and enhance weaponry to make them more precise, more intelligent and autonomous.

All of this thinking combined together would come under the concept of *weishe,* which is a combination of deterrence and compellence. "Weishe plays two basic roles: one is to dissuade the opponent from doing something through deterrence, the other is to persuade the opponent what ought to be done through deterrence, and both demand the opponent to submit to the deterrer's volition"[80]

Joint Operations

Jointness was central to waging this type of war successfully and the PLA's conception of joint operations shifted from multiple, individual

---

[79] *China's Military Strategy*. State Council, Peoples Republic of China, May 2015 at english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm (Accessed on 14 January 2021).

[80] Dean Cheng, "Chinese views on Deterrence', *Joint Forces Quarterly,* National Defense University, 2011, p.1 at https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-60/jfq-60_92-94_Cheng.pdf?ver=7wdLUCDzUSCAYlOp45xFuQ%3D%3D (Accessed on 12 February 2021).

services operating together in a coordinated fashion in the same physical space, to unified operations under a single command-and-control network.[81] This would ensure a common operational picture not only at the top but also along the entire chain of command. Having a command structure different from opposing forces was also an asymmetric advantage, adding to the confusion on the other side.[82]

MAIN AGENCIES

The Strategic Support Force (SSF) was created as part of an overall reorganization of the PLA, which resulted in the establishment of theatre commands capable of conducting full spectrum operations. The creation of the SSF was an integral part of this transformation and had large-scale ramifications for the existing organisations dealing with cyber. Like in the other militaries, space, electronic, cyber and information warfare capabilities were consolidated under this command with a view to providing C4ISR support to commanders as well as attempting to capitalise on the synergies already existing within these domains.

Creating the SSF was to be crucial to challenging future adversaries for information dominance. Once these reorganisations and changes were implemented, the PLA would have a service specifically oriented towards information warfare, including electronic warfare, network warfare, space warfare, and command-and-control warfare. It would also have a command-and-control organisation that would have developed standard operating procedures; tactics, techniques, and procedures; and more advanced doctrine and associated training standards.[83]

The Third and Fourth Departments of the PLA were relevant to cyber, respectively responsible for technical reconnaissance and offensive cyber

---

[81] Dean Cheng, no. 72, p.79.

[82] Ibid., p.33.

[83] Ibid., p..199.

operations, and equivalent to the 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 merged into the Network Systems Department (NSD) of the 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.[84] The Electronic and psychological warfare units were also incorporated into the NSD.[85]

Before the reorganisation, the management of these systems was siloed (with each answering only to its parent general department) and differentiated based on the source of intelligence collection. While the reorganization placed all these collection assets under the same organization, the 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 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. In short, the sheer breadth of what the SSF could see and hear empowered it to play a decisive role in China's comprehensive domain awareness and national defence far beyond that of any single organization that came before.[86]

Whilst the moniker SSF gives the impression that its main function is support, at the strategic level, its main goal is that of dominating

---

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

[85] John Costello, and Joe McReynolds. "China's Strategic Support Force: A Force for a New Era." Institute for National Strategic Studies, 2 October 2018 at ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf (Accessed on 15 January 2022).

[86] Ibid., p. 37.

cyberspace and the electro-magnetic 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. Therefore, providing information support and having the capabilities to conduct information warfare have become two sides of the same coin.

The re-organisation entailed simultaneous restructuring at various levels: 1) within 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 theatre commands continue to be responsible for cyber and EW operations at the operational and tactical levels."[87] By all accounts, this was sought to be achieved by first centralising all the national-level technical collection 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 theatre command." According to Cheng, "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."[88]

On the other hand, it has also been pointed out that centralisation goes against the grain of theatre commands where these commands are

---

[87] Ibid., p.43.

[88] Ibid., p.41.

supposed to be fully self-sufficient units. It would also lead to some amount of tension amongst the competing requirements of espionage, offensive and defensive capabilities and operations.

Another aspect of Chinese cyber activities is the emphasis on cyber espionage, which is an extension of information reconnaissance operations. Whilst these activities are widely known and documented and presumed to be for the purpose of exfiltrating intellectual property on innovative technologies to pass onto domestic companies, they also fulfil other goals from signalling Chinese cyber capabilities to providing an opportunity to practice skills in a real-world setting.

This reorganisation could be said to have had multiple benefits even though it would have been a painful process. It gave strategic focus to the existing capabilities which have hitherto been confined to espionage and also gave leeway to look at emerging technologies such as quantum computing, big data, semiconductors, 5G, and artificial intelligence. It also called for greater military civil fusion, which had been discussed at length in successive White Papers and military strategy papers.

The benefits of civil military fusion were that it gave the military access to innovative technologies outside of its laboratories and within the academic and start-up spaces, where the best talent resided. It also enabled the tightly controlled system to keep an eye on emerging technologies and their uses, so that there were no surprises. It was also a piece with the Assassin's Mace and asymmetric warfare approach that the military felt was necessary to provide a semblance of deterrence against the conventional and technological superiority of the US military.

However, in 2024, the almost decade-long experiment of the SSF came to an end, with the SSF being replaced by the Aerospace Force, Cyberspace Force, Information Support Force and Joint Logistic Support Force.[89] According to observers, this essentially means that,

---

[89] "PLA Information Support Force Significant in Promoting High-Quality Development of Chinese Military and Winning Modern Warfare: Commentary", *Global Times*, 20 April 2024 at www.globaltimes.cn/page/202404/1310942.shtml (Accessed on 27 April 2024).

"space operations would be delegated to the Aerospace force, cyber and electronic, psychological warfare operations would be delegated to the cyberspace force, and battlefield environment protection, information and communication assurance, and information security protection would be with the ISF."[90] The reasons for this re-organisation are yet unclear, though it is speculated that the SSF had not lived up to its mandate, and that the top leadership had become embroiled in corruption. The lessons of the ongoing Russia-Ukraine conflict could also be a factor.[91]

---

[90] Suyash Desai, "PLA SSF Scrapped, It's now the PLA ISF: What Does It Mean?" *The Economic Times*, 21 April 2024 at economictimes.indiatimes.com/news/defence/pla-ssf-scrapped-its-now-the-pla-isf-what-does-it-mean/articleshow/109476958.cms (Accessed on 27 April 2024).

[91] Ibid.

Chapter 5

United Kingdom: Restructuring through Trial and Error

Underpinnings of UK cyber posture and strategy

The UK has a long history of developing cyber strategies that address the challenges in cyberspace while also promoting technological innovation and societal progress. These strategies are derived from the National Security Strategies published over the years. The initial mention of cyber threats and their potential impacts was made in the 2008 National Security Strategy. Subsequently, in 2009, the Cabinet Office implemented its first cyber security strategy, focusing on ensuring the safety, security, and resilience of cyberspace while acknowledging its vast opportunities. This framework has served as the foundation for subsequent cyber strategies. In a 2016 ministerial statement, the following broad principles were outlined as the goal of the British cybersecurity 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 our 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.[92]

---

[92] "Final Annual Report on the 2011-2016 UK Cyber Security Strategy", 14 April 2016 at http://www.parliament.uk/business/ publications/written-questions-answers-statements/written-statement/ Lords/2016-04-14/ HLWS652/ (Accessed on 18 November 2021).

The focus on cyber threats steadily grew, culminating in the release of the UK Cyber Security Strategy, "Protecting and Promoting the UK in a Digital World," in 2011. Concurrently, the *UK Strategic Defence and Security Review* outlined a comprehensive National Cyber Security programme spanning four years, allocating a significant investment of GBP 650 million to various organisations crucial for cyber security. In 2013, an additional GBP 210 million were allocated to enhance awareness, skills, and standards. To ensure effective implementation of the objectives set forth in these documents, the government established a robust feedback mechanism.

UK CONCEPTUALISATIONS OF THREATS FROM CYBER SPACE

The UK's Ministry of Defence presented a concise overview of the cyber landscape in its *Cyber Primer*. It emphasized that the rapid expansion of cyberspace and its integration into all aspects of human life have made it an attractive domain for identifying and exploiting vulnerabilities. This created a sense of urgency for countries aiming to leverage this medium for the benefit of their citizens, organisations, private enterprises, and governance. Mitigating or overcoming these threats became crucial. However, the expansive nature of the threat landscape posed significant challenges, as the same networks were utilised by individuals, private entities, the government, and even the military. Consequently, these threats could profoundly affect the nation's government, economy, military, and industrial well-being.

While intelligence agencies, particularly those specializing in communications intelligence (COMINT), have taken up a leading role in addressing the cyber threat, there exists a tendency among them to prioritise offensive and intrusive actions rather than defence. Hostile actors have specifically targeted military networks with several objectives in mind. These include: a) gathering intelligence on the UK's military plans, b) stealing intellectual property and intelligence related to the UK's military capabilities, c) exploiting vulnerabilities within the UK with the assistance of their own military and intelligence services, d) disrupting the UK's cyberspace communications channels, e) engaging in subversive activities leveraging their intelligence services, and f) utilizing

proxies or coordinated groups to conceal the true origin of their activities within cyberspace.[93]

In an era of persistent competition, the military has to formulate a response centred on persistent engagement.[94] The United Kingdom has sought to incorporate these principles through various doctrines and approaches, including the fusion doctrine, the integrated approach, and the full spectrum approach. These frameworks envision a role for the military that encompasses its traditional responsibilities as a security provider, as well as a specific focus on cyber operations. Being the protective arm of the State, the military is granted the authority to employ force, similar to how law enforcement agencies have the legitimate right to exercise violence. Having cyber capabilities within the military's purview provides governments with a wider range of options to respond to threats effectively. Furthermore, militaries that have integrated jointness into their systems are better equipped to lead cyber responses during times of conflict, as they have prior experience in coordinating various functions. With the recognition by the United Nations that existing international laws apply in cyberspace, militaries are also better positioned to apply principles of distinction, proportionality, and discrimination within the cyber domain. Moreover, based on their existing knowledge, militaries can establish well-defined rules of engagement for cyber operations.

Another major reason given for having a clearly delineated cyber role is to encourage military personnel to incorporate cyber into their activities. Cyber operations, while currently a niche area, are mainstreaming rapidly as militaries operate in and through the cyber domain in conjunction with the maritime, land, air and space domains. Mainstreaming cyber in the military will increase cyberspace awareness,

---

[93] *Cyber Primer: Second Edition*, Ministry of Defence (UK), 20 July 2016 at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160 720-Cyber_Primer_ed_2_secured.pdf, page 32 (Accessed on 15 December 2021).

[94] Phil Lester and Sean Moore, "Responding to the Cyber Threat: A UK Military Perspective", *Connections,* 19 (1), 2020, p.40.

agility and utility by generating war fighters capable of operating in cyberspace rather than producing cyber warriors. [95] Furthermore, this approach addresses an additional challenge faced by modernizing militaries—the need to coordinate among different teams within their own ecosystem. In the context of cyber operations, this includes teams involved in electronic warfare systems, signal intelligence, and the management of communication and information systems. It is crucial for each team to have a comprehensive understanding of the functions performed by the others, enabling closer integration and interaction. Traditionally, militaries have not been accustomed to coordinating efforts outside their domain. However, in the realm of cyber command and control, close collaboration with multiple agencies and even international partners is essential. Additionally, coordination with the private sector adds further complexity to the equation, as issues of secrecy must be addressed and resolved.

The military faces threats not only to its own internal networks but also to those of its suppliers, specifically within the defence industrial complex, including subcontractors involved in procurement, logistics, and support functions. These suppliers, even smaller-medium sized companies, are vulnerabilities as they often lack sufficient resources to invest in robust cybersecurity measures. Consequently, they become regular targets for attacks. Moreover, the interconnectedness of critical information infrastructure introduces the possibility of successful attacks originating from unexpected sources, with potentially unforeseen consequences.[96]

Nevertheless, the most significant challenge faced by militaries lies in defining their role within the cyber domain. Policy makers and strategists have attempted to address this complexity by employing the concept of concentric circles or, in the case of the UK military, by categorizing operating spaces as near, mid, and far. The "near" space encompasses networks and systems directly controlled by the military, while the "mid"

---

[95] Ibid., p.42.

[96] *Cyber Primer: Second Edition*, no.93, p.11.

space includes critical infrastructure networks and systems that are not under the direct control of the military or other State agencies. The "far" space comprises networks and systems owned by third parties, which may even be located outside the country.[97] However, it is important to recognize that civilian and military cyber infrastructure cannot be clearly delineated and often overlap in practice.

Main Agencies

At the highest level, the responsibility and accountability for cyber security initially resided with the Home Office. However, due to the growing necessity for effective coordination, this responsibility was transferred to the Cabinet Office. Within the Cabinet Office, cyber security falls under the purview of the National Security Council Secretariat, and coordination is facilitated 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 the Government Communications Headquarters (GCHQ) had the responsibility to "develop capability to detect and analyse cyber threats, pre-empt attacks and track down those responsible".[98] This was a natural progression considering that the GCHQ, with its extensive history in signals intelligence dating back to 1919, has maintained its leadership position and capabilities over the years. Traditionally, the GCHQ reported to the Secretary of State for Commonwealth and Foreign Affairs, and its main clients included the Ministry of Defence, the Foreign and Commonwealth Office, as well as law enforcement and intelligence agencies such as MI5, and MI6. With a staff estimated to exceed 5,000 employees and the largest portion of the single intelligence budget (around GBP 2.2 billion in 2021), the GCHQ's operations were shrouded in secrecy. However, some of its activities have been publicly

---

97 Ibid.

98 "National Security Strategy and Strategic Defence and Security Review." 2015 at https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015 (Accessed on 12 November 2021).

acknowledged, such as a "major offensive cyber campaign" conducted in partnership with the Ministry of Defence against ISIS.[99]

According to John Ferris, the official historian of the GCHQ and author of the book *Behind the Enigma: The Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency*, a significant shift occurred in the GCHQ's role following the end of the Cold War. For the first time in its history, the GCHQ was tasked with combating major threats and had evolved into a fighting service of its own. In 1938, the ratio of soldiers to signal intelligence personnel stood at 200 to 1, whereas by 2020, it had reduced to 14 to 1. This transformation in role and increased visibility necessitated a shift from a secretive intelligence agency to a more publicly engaged entity.

As a result, the National Cyber Security Centre was established, drawing inspiration from Israeli efforts to foster a nurturing ecosystem. Both the parent organization, GCHQ, and the National Cyber Security Centre were mandated to prioritize research and development while sharing information with the private sector. A cyber accelerator programme was created to support start-ups, granting selected companies access to the GCHQ's technological capabilities. The GCHQ also played a role in training cyber security professionals by identifying young talent from schools, and even offering a GCHQ certified master's degree in cyber security.[100] Despite these efforts, the public facing 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.

On the military side, there was a requirement for the military also to be plugged into this space, since they were in the crosshairs of hostile actors for the reasons mentioned earlier. The Ministry of Defence developed a joint cyber group to integrate the capabilities within the

---

[99] Jeremy Fleming, "Director's speech at Cyber UK 2018", CyberUK18, 12 April 12, 2018 at https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018 (Accessed on 18 October 2021).

[100] Melissa Hathaway, et al, *United Kingdom Cyber Readiness at a Glance*, Potomac Institute for Policy Studies, October 2016, p.11.

MoD primarily to defend its networks but also to have on-hand capabilities to assist other agencies when the need arose.[101] The creation of the Joint Forces Cyber Group in 2013 resulted in the establishment of two separate joint cyber units, one dedicated to defensive capabilities and the other to offensive capabilities. In 2018, the Ministry released the Joint Doctrine Note (JDN) 1/18 on Cyber and Electromagnetic Activities, which defined cyber operations as the planning and coordination of activities in and through cyberspace, aimed at enabling freedom of manoeuvre and achieving military objectives. According to the JDN, cyber operations were categorized into four distinct roles: offensive cyber operations, defensive cyber operations, cyber intelligence, surveillance, and reconnaissance (ISR), and cyber operational preparation of the environment. These categories encompassed the diverse functions and activities required to effectively operate in the cyber domain as part of military operations.[102]

Each of these roles had a certain level of complexity, even within the services. For instance, for the Navy, at the platform level, new platforms depended on "a multitude of network systems including communication, navigation, propulsion, life support (water, waste, etc.) and weapons." Vulnerabilities in these systems posed a significant risk to operational effectiveness.[103] Naval platforms often encountered bandwidth challenges while operating at sea, leading to difficulties in distributing patches and software updates, unlike the situation on land.

---

[101] Ibid., p.10

[102] 'Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities', Ministry of Defence (UK), February 2018 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, p.32 (Accessed on 18 January 2022).

[103] Christopher Argles, "A Conceptual Review of Cyber-Operations for the Royal Navy" *Cyber Defense Review,* 18 December 2018 at https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Summer%202000/CDR%20V5N2%20Summer%202020-r8-1.pdf (Accessed on 18 October 2020).

To address this issue, the implementation of three-level cyber protection teams was introduced and deployed with each platform, taking into account the platform's size and threat assessment. Level three protection teams were specifically designed as quick response units that could be deployed when needed.

For the military, the primary challenge lies in securing its own networks. Both critical military infrastructure and military platforms are vulnerable to cyber attacks, both in times of peace and during wartime. Safeguarding these networks is crucial to ensure the integrity and reliability of military operations.

Most of the recruits for the new cyber divisions came from the information warfare division. A maritime cyber reserve had also been established in 2014, which drew recruits from the private sector. Physical entry requirements were relaxed for these recruits. Among the more useful training tools were Capture the Flag (CTF) exercises.

> "CTF consists of at least two networked teams in competition against one another. Each team owns a server with known vulnerabilities, on which resides a data file (the flag). To score points, a team must compromise the server of an opponent and replace the flag with their own. At the same time, the team must defend their network and prevent their flag from being compromised. An independent server monitors the network and scores teams for successful offensive and defensive CO. To encourage teams to think cleverly about their actions, the score server places a fine on bandwidth usage."[104]

The National Cyber Force

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,

---

[104] Ibid., p.13.

1st (United Kingdom) Signal Brigade, 11th Signal Brigade & HQ West Midlands and 77th Brigade. In 2019, the Force Troops Command was renamed as the 6th Division.

November 2020 saw the merging of these two tracks with the establishment of the National Cyber Force (NCF) with personnel drawn from the GCHQ, the Ministry of Defence, the Secret Intelligence Service (SIS/MI6) and the Defence Science and Technology Laboratory (DSTL), with the units' funding coming from the Ministry of Defence. 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."[105] The justification 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.[106] The establishment of the NCF has sparked questions regarding its specific focus and objectives. There is ambiguity regarding whether the NCF's primary aim is to dismantle the infrastructure of ransomware cyber criminals, conduct counter-cyber operations against hostile State actors, or prepare for and engage in military operations.

The 2022 National Cybersecurity Strategy states that the UK intends to utilise the capabilities of the NCF more frequently to disrupt threats from both State and non-State actors, thereby supporting the country's broader national security interests. This emphasis on routine use of the NCF's capabilities suggests a potentially more aggressive role, which has raised concerns about the potential for increased instability in cyberspace rather than less.

Finding the right balance between offensive cyber operations and maintaining stability and security in cyberspace is a complex challenge.

---

[105] Marcus Willet, "Why the UK's National Cyber Force is an important step forward", *IISS Analysis*, 20 November 2020 at https://www.iiss.org/blogs/analysis/2020/11/uk-national-cyber-force (Accessed on 18 November 2021).

[106] Ibid.

It is crucial to carefully consider the potential risks and unintended consequences associated with an increasingly assertive cyber posture. Oversight and strategic planning are essential to ensure that the NCF's actions align with the goal of enhancing national security while minimizing potential negative impacts on overall stability in cyberspace.

Chapter 6

Israel: Absent Cyber Command

Underpinnings of Israel's Cyber posture and strategy

Israel presents a fascinating study in cyber warfare. It has been perpetually in a state of heightened readiness since it is surrounded by hostile neighbours. The advent of cyber warfare has presented new challenges to Israeli policy makers, but they have seized upon it as an opportunity to build on Israel's traditional strengths in technology and their application in the military, to become world leaders in utilising cyber to augment the traditional strengths of the military.

Israel has faced a range of security threats since the major conflicts of the 1960s and 1970s. These threats have largely been hybrid in nature, encompassing conventional low-intensity and asymmetrical challenges from various groups, as well as regional-level dangers such as weapons of mass destruction, missiles, and now cyber threats. In response, Israel has primarily relied on deterrence and retaliation strategies to counter these threats. However, the emergence of cyber threats has introduced new uncertainties and challenges to security.

Developing comprehensive security plans has become increasingly complex for security planners, tasked with creating short, medium, and long-term strategies. They face numerous challenges, especially in rapidly evolving technological landscapes. This includes evaluating operational requirements, prioritizing weapon technologies, and forecasting the types of threats the country may encounter. Moreover, an even greater challenge lies in continuously reforming and reorganising the military's structure to address future needs while maintaining its ability to address immediate challenges.[107]

---

[107] Michael Raska, *Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy,* S. Rajaratnam School of International Studies, Singapore, 2015, p.3.

Israel has positioned itself as a leader in the field of cybersecurity, capitalizing on its early adoption of a well-defined policy and swift implementation. This proactive approach has yielded successful outcomes, establishing a foundation of best practices that subsequent governments have built upon. Israel has not only utilised these achievements to enhance its national cybersecurity but also leveraged them for cyber diplomacy, demonstrating its expertise and accomplishments to the international community. In doing so, Israel has offered to share its knowledge and experiences as a means of garnering positive recognition and appreciation.

The roots of Israel's cybersecurity policy can be traced back to the strategic principles laid out by David Ben Gurion, the nation's founding father and first Prime Minister. These principles encompassed the defence of the State, protection of its infrastructure and interests, deterrence against potential attacks, forming alliances with powerful nations, and the development of advanced early warning capabilities. By drawing inspiration from these doctrines, Israel's cybersecurity policy aligns with its broader strategic outlook, compensating for its lack of strategic depth and ensuring the safeguarding of its national interests.[108]

Taking into consideration the evolving nature of warfare, Israel has devised a concentric circle approach to its military commitments. These commitments are structured around three key areas: the immediate perimeter, intra-frontiers, and remote regions. Recognizing the expanding influence of cyberspace, which has permeated every aspect of political, military, and socio-economic domains, Israel has acknowledged the emergence of a new battleground comprising cyber and information technologies.

Adversaries have seized upon the advantages presented by these domains, employing asymmetric warfare tactics to target critical infrastructure without fear of immediate retaliation, mainly due to challenges associated with attribution. Israel's policy planners have also

---

[108] *Israel's National Cybersecurity and Cyberdefense Posture*, Center for Security Studies (CSS), ETH Zurich, 2020, p.13.

recognized that, as a nation in a constant state of conflict unlike many others, this perpetual conflict would extend into the realm of cyberspace as well. Consequently, a pattern of alternating periods of relative peace and military operations on the periphery, followed by retaliatory actions, is expected to manifest in cyberspace as well.[109]

Background

As early as 1997, the Tehila unit was established. It was "charged with coordinating [S]tate infrastructure and increasing productivity, efficiency, and security throughout the government." However, this initiative only had mixed success with most agencies not bothering to coordinate with this unit. The 9/11 attacks in the United States in September 2001 prompted a fresh study of threats to the homeland and cyberspace domains, seen as a medium through which a similar surprise attack could take place.[110] In 2002, the National Security Council was tasked to "outline strategies for emerging risks". This resulted in a focus on critical infrastructure protection and a national cyber security policy. The Ministerial National Security Committee Resolution 84, regarding "responsibility for protecting civilian computer systems", was passed, which provided the framework for the national critical computer systems policy. This defined 19 critical systems and was structured so that the primary responsibility lay with individual organisations, which also had the responsibility to share information with the relevant ministry of the government under which it served. This resulted in considerable fragmentation of authority and responsibility.[111]

In 2010, a committee was formed to review existing policies and recommend new ones and a national plan for cyber security. The committee comprised eighty experts from the various ministries, the military and academia. The committee, a national task force, was created with the objective of coming up with recommendations to ensure that

---

[109] Michael Raska, no.107, p. 4.

[110] Dmitry (Dima) Adamsky, "The Israeli Odyssey toward its National Cyber Security Strategy", *The Washington Quarterly,* 40 (2), 2017, pp. 113-127, p.4.

[111] Michael Raska, no.107, p.8.

Israel became one of the five leading countries in cyberspace.[112] It had the stated goal of "preserving Israel's international status as a center for the development of data technologies and to provide the country with powerful capabilities in cyberspace to the end of ensuring Israel's economic and national resilience as an open and democratic knowledge based society."[113] Based on these recommendations, the Government Resolution 3611, the equivalent of an Executive Order, was promulgated. [114]

Resolution 3611 focused on critical national infrastructure protection and creating new organisations towards this end, with adequate powers and responsibilities. The overall aim was to advance national cyber capabilities. To this end, a National Cyber Bureau (NCB) was established within the Prime Minister's Office in 2012. The Bureau's mandate was "to formulate comprehensive and formal cyber strategy, to articulate and lead national cyber policy, advise the government on cyber matters, advance R&D in academia, the educational system, and industry; develop cyber-technology as an economic growth engine; and leverage cyber security for international cooperation."[115] In addition to having responsibility for cyber policy issues and coordination, it also facilitated interaction between actors outside of Government such as academia and the private sector. It was also given the mandate of coordinating agencies within the Government, the different Ministries, and the national security agencies, including the Israel Defense Forces, the Israeli Security Agency (ISA), the Mossad, the police force and the "director of security of the defence establishment, unit within the defence ministry".[116]

As seen in other parts of the world, there was opposition from the established agencies. Shin Bet, the internal security agency, claimed that

---

[112] *Israel's National Cybersecurity and Cyberdefense Posture*, no.108.

[113] "Advancing National Cyberspace Capabilities Resolution No. 3611, Government of Israel, 7 August 2011, Unclassified," National Security Archive at nsarchive.gwu.edu/document/22530-document-05-government-israel-resolution-no. (Accessed on 17 October 2020).

[114] Elena Chacko, "Persistent Aggrandizement? Israel's Cyber Defense Architecture", Aegis Series Paper No. 2002, 2020, p.3.

[115] Dmitry (Dima) Adamsky, no.110, p.5.

[116] Elena Chacko, no.114, p.2.

the NCB would be unable to carry out its mandate because it lacked intelligence-gathering capabilities, had no operational tradition and no possibility of integration with similar security organisations worldwide.

As a consequence to this, in 2015, Resolution 2444 was released which led to the establishment of the National Cyber Security Authority (NCSA), which was to work side by side with the National Cyber Bureau. While the National Cyber Bureau was responsible for the "overall strategic policy planning in the realm of capacity building", the National Cyber Security Authority, was responsible for the national-level implementation and regulation. The expectation was that the authority would pick up capabilities to prevent cyber-attacks and address threats. To this end, it was provided with access to cyber intelligence and analysis from across the various national security agencies. Its mandate was to issue guidelines, regulate cyber security services and guide the work of "cyber security units within government ministries."[117] This Resolution also provided for the establishment of a national Cyber Emergency Response Team (CERT) which would "provide assistance in cyber defense, facilitate information sharing, can allow for coordination between security agencies and other actors." CERT was to also include the National Incident Management Center, which would handle "reports on cyber-attacks vulnerabilities, and security breaches."[118] The Authority began operations in 2016 and those of CERT started in 2017.

In 2018, all these agencies were merged with the new National Cyber Directorate set up "due in part to overlapping authority and bureaucratic redundancies between the Bureau and the authority under the original framework."[119] According to Elena Chacko, the main issue was that of overlapping authority not just between the new agencies, but also

---

[117] "Government-Resolution-No-2444- Advancing the National Preparedness for Cyber Security", Government of Israel at ccdcoe.org/uploads/2019/06/Government-Resolution-No-2444-Advancing-the-National-Preparedness-for-Cyber-Security.pdf. (Accessed on 18 January 2022).

[118] Elena Chacko, no.114, p.3.

[119] Ibid., p.3.

between the new and existing agencies such as the Israeli Security Agency (ISA the internal security service, colloquially known as Shabak) and the transfer of existing authorities to these new agencies.[120]

The National Cyber Directorate (INCD) was to be the "the highest national authority for strategic cyber policy planning, for the regulation of its operational execution across the government, and for building cyber capabilities for the short, medium, and long term."[121] The National Cyber Bureau and the National Cyber Security Authority were subsumed within it. The Directorate was also made responsible for international cooperation, and creating and updating the existing legal frameworks. Co-ordination with the military was also another responsibility and to that end, the creation of mechanisms to fill the gaps in coordination. Finally, it was also mandated to come up with unified threat projections to "improve situation analysis capabilities for intelligence services and stakeholders." Whilst the INCD had the responsibility for coordination of cyber at the national level, during times of war or national emergency, that role was to be taken over by the Israel Defense Forces. The 2019 budget for the INCD was estimated to be between US$ 32 and 64 million, with a staff strength of about 250.[122]

The creation of the INCD has still not removed the underlying tensions over distribution of responsibilities. According to Frei, "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."[123] The existing distribution of responsibilities was also intricately tied to Israel's history. For instance, the reason behind Shin Bet having responsibility for critical infrastructure protection was that the Israeli government had to quickly assign the responsibility during the "high-tension period

---

120 Ibid., p.3

121 Dmitry (Dima) Adamsky, no.110, p.9.

122 *Israel's National Cybersecurity and Cyberdefense Posture*, no.108, p.15.

123 Ibid., p.15.

of the Second Intifada (2000-2005)."[124] This was not sustainable since intelligence agencies had much lower levels of oversight and responsibility. These efforts notwithstanding, the intelligence agencies, Shin Bet and Mossad continue to operate 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."[125]

Efforts to codify the Government Resolutions through legislation have been underway for quite a few years now, culminating in the release of a draft Cyber Defence and National Cyber Directorate Bill in 2018. According to Elena Chacko, the draft centred around three key policy principles: "the need for a concerted national response, facilitating cooperation between government and the private sector, and preserving the authorities and responsibilities of the 'old' national security establishment."[126] The submission of the Bill saw a tussle between the various agencies, with the intelligence agencies even submitting their objections in writing. As a result, it was specified that the INCD would have responsibility and oversight only for "identifying, containing, and analyzing cyberattacks within Israel, with the response to the attacks being directed by other competent authorities. Furthermore, the Bill also provided for "the ISA to assume the directorate's powers when a cybersecurity threat is related to counterterrorism or espionage."[127] The exceptions specified within the Bill for national security purposes and to keep the security agencies outside its purview, made it a paper tiger since much of these activities took place in a domestic environment. These lacunae resulted in controversies such as the Pegasus scandal unfolding in the subsequent years.

On the military side, there were attempts to comprehensively reorganize and create a unified cyber command around the same time. The existing

---

[124] Ibid., p.10

[125] Ibid., p.15

[126] Elena Chacko, no. 114, p.4.

[127] Ibid., p.4.

organisations within the military comprised 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."[128] However, that plan was shelved for reasons that are unclear. The Israel Defense Forces also brought out a public defence doctrine in 2015, which incorporated cyber into the overall strategy, effectively declaring cyberspace as the fifth domain of warfare. Quite comprehensive for its time, the strategy looked at cyber in its role as a support function as well as its use for offensive and defensive purposes, "at all levels of combat (i.e. strategic, operative, and tactical)."[129] Creating capacities equally in all these areas were seen as essential to "the functioning of the state and IDF institutions, the utilization of intelligence, collective defense, 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 stage 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 defense command and control."[130] However, the main goal of creating a Cyber Command was stillborn, even though it was announced by the then Chief of Staff Gen. Gadi Eizenkot.

The Central Collection Unit of the Intelligence Corps or Israeli SIGINT National Unit (ISNU), more commonly known as Unit 8200, is responsible for offensive cyber warfare. 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.

Stuxnet was directed against the Iranian nuclear programme, and suspicions of US and Israeli involvement were confirmed by subsequent

---

128 Ibid., p.4.

129 Ibid., p.9.

130 Michael Raska, no. 107, p.11.

reports. These suspicions arose in the first place because of the sophistication of the malware, which, experts declared, could only be engineered through the resources available to a nation state. It was the first large-scale attack on critical infrastructure that ran on Supervisory Control and Data Acquisition (SCADA) systems. The Duqu, Gauss and Flame malware were deemed to be part of the same malware family but unlike Stuxnet, their primary purpose seemed to be espionage, with their targets ranging from banking to governmental and energy networks. Flame, in particular, was notable for its modular character and its size, averaging 20 MB. Its capabilities ranged from recording Skype conversations and downloading information from smartphones to more mundane activities such as recording audio, screenshots, keystroke, and network traffic recording.

These malwares could be created because Unit 8200 was backed up by virtually unlimited resources, and given a *carte blanche* to engage in sabotage of enemy industrial facilities, carry out cyber espionage and undertake other actions to support the military forces. It is estimated that the Unit had as many as 5000 personnel and was the largest of its kind in the IDF.[131] It has also benefited from a close association with the US National Security Agency (NSA), with the agency giving it access to the information that it collects through its worldwide signal intelligence collection network. Collaboration is not just limited to data sharing but also technical expertise, "information on access, intercept, targeting, language, analysis and reporting."[132]

The cyber ecosystem that subsequently became a model for State-private sector partnership, was also beginning to take shape at this time. Unit 8200 took advantage of the four-year compulsory military

---

[131] Sean Cordey, *The Israeli Unit 8200 An OSINT-based study*, ETH Zurich, December 2019, p.4

[132] Ibid., p.11 quoting G. Greenwald, L. Poitras, E. MacAskill, 2013. "NSA shares raw intelligence including Americans' data with Israel", *The Guardian*, 11 September 2013 at https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents (Accessed on 28 November 2020).

service for Israelis to select promising students based on their analytical capabilities and train them in cyber technologies. Many of these youngsters then went onto work or founded cyber-security start-ups, leading to Israel being given the moniker of the start-up nation. The IDF can also call on them when required due to the mandatory reserve duty requirement for up to three weeks every year until the age of 50.[133] A final point in favour of the success of this ecosystem was that they tended to maintain a social network that created strong links between the private and public sector, military, and the intelligence community.[134]

The creation of Israel's cybersecurity ecosystem has evoked much interest in other countries that sought to replicate Israel's success in this area. However, as has been brought out by many analysts, in addition to the factors mentioned above there are a number of historical reasons for this. Much of the credit goes to Israel's first Prime Minister who recognised that Israel was surrounded by hostile neighbours and seized on achieving technological superiority to compensate for this.[135] Right from the time the IDF was created there has existed a science corps within it.[136] Another factor was the sociological construct of Israeli society; particularly the kibbutz system with its emphasis on sharing, which converted to meetups, hackathons, lectures, training sessions and co-working spaces which facilitated the sharing of knowledge.[137] For its part, the IDF did not insist on acquiring intellectual property rights on products developed during military service, thus allowing knowledge to be transferred to the private sector.[138]

---

133 Sean Cordey, no. 131, p.15.

134 *Israel's National Cybersecurity and Cyberdefense Posture*, no. 108, p.15.

135 Gil Baram and Isaac Israel, "The Academic Reserve: Israel's Fast Track to High-Tech Success", *Israel Studies Review*, 2019, p.7.

136 Ibid. p.8.

137 Ibid. p.6

138 Ibid. p.4

C4I Directorate

The other unit within the military responsible for cyber defence is the C4I Directorate. Its main concern is the protection of the IDF's networks. It operates on the doctrine of Active Cyber Defence, i.e., deterring and pre-empting attacks by proactively monitoring adversary activity, to the extent of sitting in their networks in order to have early warning of impending attacks.[139]

Israeli army doctrine

The national cybersecurity strategy of 2017 laid out the defensive and offensive responsibilities of the IDF. The strategy was based on the overall guiding principles that have helped Israel's defence since its inception. These principles, laid down by David Ben Gurion, included deterrence, ensuring decisive victory, early warning, and alliances. With regard to the first, the example given is Israel reacted in real time to a cyber-attack by Hamas and bombing its cyber headquarters as a retaliatory measure in 2019.[140] Whilst some elements of the overall strategy have been incorporated into the cyber doctrine, others are less easy to incorporate. Whilst deterrence would call for immediate tit-for-tat actions of the example given above; this has proved to be more the exception than the norm, since cyber-attacks are too numerous to entail such a continuous response. Thus, the emphasis seems to be more on developing and optimizing 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 INCD is in charge of managing national

---

[139] *Israel's National Cybersecurity and Cyberdefense Posture*, no. 108, p.16.

[140] Zak Doffman, "Israel Responds to Cyber Attack with Air Strike on Cyber Attackers in World First", *Forbes*, 6 May 2019 at https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first (Accessed on 15 January 2021).

cyber defence. During times of emergencies, the IDF coordinates offensive and defensive cyber campaigns at the national level.[141]

Whether this framework will stay viable or whether there will be a move towards the creation of a Cyber Command, its role from a military perspective, attendant issues such as nature and extent of cooperation with civil agencies, etc. are all debates waiting to happen.[142]

The military's influence on cyber policy is evident in the appointment of former Israeli Defense Forces (IDF) officers with operational experience in cyber, to key positions within the Israeli National Cyber Directorate (INCD). This strategic decision ensures that individuals with first-hand knowledge of cyber operations and defence are at the helm of shaping cyber policies. Eviatar Matania, the Founder Director of both the National Cyber Bureau and the Israeli National Cyber Directorate, possessed extensive experience in both the IDF and the private sector. Similarly, his successor, Buky Carmeli, previously held the position of Head of the Ministry of Defence's cyber and technology defence authority. Following Carmeli, Yigal Unna assumed leadership, bringing with him a background in Unit 8200, Israel's elite intelligence unit, and experience as the Head of the Cyber Warfare Unit in the Shin Bet, Israel's internal security agency. The current Head, Brigadier General Gaby Portnoy (Retd.), served an impressive 31 years in military intelligence, including as the Head of Operations in the Intelligence Corps. By appointing individuals with military backgrounds and extensive intelligence expertise to key positions, Israel ensures that its cyber policy is shaped by individuals who possess a deep understanding of the operational aspects and complexities involved in cyber defence and warfare.[143]

---

141 *Israel's National Cybersecurity and Cyberdefense Posture*, no. 108, p.17

142 Ibid.

143 "Israel appoints ex-general as head of government cyber security", Reuters, 20 February 2022 at https://www.reuters.com/world/middle-east/israel-appoints-ex-general-head-government-cyber-security-2022-02-20/ (Accessed on 20 February 2022).

This also facilitates the smooth operation of inter-agency initiatives such as cyber training exercises and simulations of cyber attacks between the IDF, INCD and other agencies.[144] The IDF has put a lot of emphasis on simulations creating virtual cities consisting of "residential and commercial neighborhoods, railway, airport, electric grid, nuclear reactor, stock market, military base, and missile defense system."[145]

The absence of a cyber doctrine and the Cyber Command, a result of internal disagreements, could have reduced its potency to contribute to Israel's warfighting capabilities. Cyber capabilities are present but there seems to be very little integration at the tactical and operational levels in the military, and they seemingly exist as a standalone capability. However, there is always more than meets the eye when it comes to the functioning of the Israeli military.

---

[144] Charles D. Freilich et al, *Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power*, 2023 (online edn.), Oxford Academic, 22 June 2023, p.197.

[145] Ibid.

Chapter 7

Conclusion

This study of the role of the military in cyberspace with particular emphasis on the evolution of its role in five countries that are considered cyber powers with capacities and capabilities not available to other powers brings many different aspects to the forefront. The resources, capabilities, authorities, and partnerships needed to conduct cyberspace operations has been the focus of this Monograph. It has examined the existing structures, resources, capabilities and authorities of the militaries in five countries. In those countries where the military intelligence agencies were the nodal agencies for cyber, the military had a greater role to play. This was the case with the United States and the National Security Agency, with the British GCHQ, as well as with the various military agencies in China which were subsequently folded into the Strategic Support Force. Where lines of authority were not so clearly demarcated as in the case of Russia and Israel, the military initially played a subordinate role, and subsequently asserted itself. However, their roles in these countries are still being worked out, as existing agencies are reluctant to give up their influence. It is instructive that in these countries, a Cyber Command is yet to be formalised, though there have been unsuccessful attempts to do so in Israel. The same is true for the United Kingdom, but what has been established through the national cyber force is a Cyber Command, to all intents and purposes.

It is a given that cyber war in the classic sense is yet to take place. What we see today are cyber skirmishes with temporary rather than permanent effects. If you take the outcomes country by country, in the case of the United States, its sheer technological prowess makes it virtually impossible to identify attacks in the cyber domain by its military except when it chooses to make those attacks known. China also has on the face of it, kept away from destructive cyber-attacks even though it is central to its military doctrines and strategies. Russia has used its cyber

weapons and capabilities as part of its overall strategy in the various wars it has conducted over the past 20 years. While it was a strategic game changer in the initial years since the opposing sides were caught unawares by cyber-attacks, the balance has subsequently equalised to an extent and Russia has found itself on the receiving end of cyber-attacks since it has a huge cyber landscape. This is despite efforts to strengthen defence by a policy of deterrence through denial. Israel also started in a leading position and has maintained that position and become a pioneer in cyber defence technologies but continues to be laid low by lower-level cyber-attacks from actors hostile to it without adequate possibilities to respond in kind since the opposing sides have very few cyber-enabled targets.

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 to be ready for cyber conflict. However, their role is yet to be clearly defined as seen in the questions around the role of the British National Cyber Force. Russia has been pilloried for being at the forefront of carving out treaties and norms on cyberspace while flouting many of these norms in its efforts 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 cyber conflict. The threat landscape is too vast for effective denial and the attacks are too numerous for a policy of deterrence by punishment.

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, there is the nature of the organization itself with a number of different agencies offering different competencies that 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 complications when it comes to re-alignment of organisation, recruitment of personnel, and working with other actors in the civilian space.

The cyber environment has proved to be much more complicated and multi-dimensional, and therefore, while the objectives in both electronic and cyber warfare, viz., "Deny, deceive, disrupt, destroy, or exploit the adversary's capability to communicate, monitor, reconnoitre, classify, target, and attack" might be similar, it is not as easy to follow through on these objectives in cyberspace. 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 supported the other domains, and not a major theatre of conflict in itself. The rapid evolution of this domain has also resulted in a haphazard allocation of responsibilities, with different organisations taking responsibility for managing and utilising different aspects of the domain at different points in time. Intelligence organisations, either from the civilian or the military stables, became de facto leading agencies by virtue of the fact that much of State-sponsored activity has revolved around cyber exploitation, viz., espionage and related activities. Policy makers have been unable to take a decision on giving the dominant role to any one organisation. The transition to other agencies has proved 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.

Militaries have traditionally conducted their operations guided by the principles of proportionality, necessity, and distinction. However, these principles present significant challenges when applied to cyber-attacks in a cross-domain context. These have been also the subject of undertakings such as the Tallinn Manual, which has studied the use of force in cyberspace and the application of international law to cyber conflicts and cyber warfare. As this study has shown, relying on very narrow classic definitions of war and weapons would make it very difficult to flesh out the military's role.

The domination of the deterrence paradigm has been seen as responsible for the description of cyberspace as the Fifth Domain of warfare, which led to expectations that doctrines that had proven successful in the other domains could easily be adapted to this domain. Attack artefacts like source and intent and concepts like signalling and escalation dynamics which worked well in the physical domains to

pinpoint attack and responses, did not lend themselves well to the cyber domain. This has sought to be countered through other formulations that have come up in academic writings. One such alternate strategy has been that of "cyber persistence" to both engage in, and respond to, other States' "operations, activities and actions" in cyberspace. Much of this now forms the academic underpinning of the changed US policies of persistent engagement and forward defence.

The Chinese military conceptualised cyberspace as an arena of continuous warfare and reformed their military in 2015, setting up new Forces, with the Strategic Support Force incorporating infamous units like PLA Unit 613998 within itself. This conceptual integration of peacetime and wartime was expanded through other concepts such as "military civil fusion" and "pre-emptive cyber-attack". Russia's is a similar case. Russian and Chinese authored articles are notable for emphasising that most offensive actions attributed to them are in fact defensive actions. On the other hand, Western authors try to highlight the fact that responses by the Western countries are a result of aggressive actions by the Chinese and the Russians. Thus, the fog of cyberwar is leading to escalatory actions which are themselves quite opaque.

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 have to take the initiative in carving out their roles in the cyber verse, instead of having it laid out for them. Even if it plays havoc with existing structures and doctrines, conflict in cyberspace cannot be wished away, and militaries have an increasingly important role to play in this new domain.

Whilst there has been discussion in policy circles and within the Indian military on creation of a cyber structure and enhancement of existing cyber capabilities within the Armed Forces, progress on this front has been incremental. A Defence Cyber Agency was created in 2019 based on the recommendations of the 2011 Task Force on National Security, popularly known as the Naresh Chandra Committee. It was composed of personnel from all the three services and led by a Vice- Admiral. Given the increasing importance of cyberspace, it was widely expected that this would be an interim organisation, which would be subsequently

scaled up to a Cyber Command, incorporating all the disparate agencies dealing with cyberspace and electronic warfare within the military. These expectations have been belied with further fragmentation, rather than consolidation, happening subsequently.[146] Though a joint cyber doctrine was brought out in 2024, it has not been made available in the public domain, thus reducing its deterrent value.[147]

The various doctrines published so far only refer to cyber in passing and in generic terms. The most recent of the doctrines, the *Air Force Doctrine* of 2023 simply notes that:

> Adversaries have adopted grey zone tactics by employing cyber, information and economic means as instruments of statecraft. These challenges constitute a widened spectrum of conflict, from relative peace marked by sub conventional attacks, escalating to low intensity conflicts and finally total war. The nation is faced with challenges that require adaptive strategies. We need to be proficient in conduct of warfare in Land, Air, Maritime, Space, Cyber, EW and IW domains simultaneously at the Strategic, Operational and Tactical levels.[148]

Doctrines brought out by the Navy (2015), the Army (2018) and the Integrated Defence Staff (2017) have had inputs on similar lines. *The Joint Doctrine of the Indian Armed Forces,* brought out by the Integrated Defence Staff, from its perspective, referred to cyber primarily as an enabler and a support to the main mediums through which wars were to be fought.[149]

---

[146] "Army decides to operationalise Command Cyber Operations & Support Wings"*, India Today,* 27 April 2023 at https://www.indiatoday.in/india/story/army-commanders-conference-pointers-command-cyber-operations-and-support-wings-2365319-2023-04-27 (Accessed on 15 May 2023).

[147] Press Information Bureau, CDS Gen Anil Chauhan releases Joint Doctrine for Cyberspace Operations https://pib.gov.in/PressReleasePage.aspx?PRID=2026240 (Accessed on 24 June 2024).

[148] *Doctrine of the Indian Air Force*, 2023, p.73 at https://indianairforce.nic.in/wp-content/uploads/2023/01/2MB.pdf (Accessed on 15 May 2023).

[149] Integrated Defence Staff*, Joint Doctrine Indian Armed Forces* (2017), p. 48 at https://ids.nic.in/WriteReadData/Document/2/13/1718bbb2-cb9c-4ef5-9843-cb670e58afb7.pdf (Accessed on 19 June 2023).

It is evident from the foregoing case studies that forging the development of a specific Indian cyber doctrine and building up the required capabilities will be a long-drawn-out task. With the Defence Cyber Agency having been in existence since 2021, an in-depth study needs to be undertaken of what it has achieved so far and what needs to be done to empower it further. If it is to continue in its present state, it should focus on three aspects: 1) creating a joint cyber doctrine; 2) undertaking scenario building, simulation exercises and building up forward planning of capabilities; and 3) creating the kernel of a future cyber corps that is not dependent on the existing services and gives avenues for civilian participation on the lines of the US *Cyber Service*. Creation of cyber doctrines also entails study of the cyber doctrines of other powers, particularly of inimical ones, their capabilities, their declared intent as well as operations carried out, and trace them back to these powers.

At the moment, a certain amount of complacency seems to have set in, in the absence of any major attacks and the defence cyber agency seemingly providing an adequate set of capabilities for the armed forces. However, this might be predicated on the low-level cyber-attacks, which are easily defended. India, like the other countries, is highly cyber-dependent and has to be better prepared in terms of strategy to respond to higher-level attacks. Indian military cyber strategies seem closest to the Israeli model; there is no Cyber Command, nor a comprehensive strategy and the head of the apex body coordinating cyber security hails from military background. However, it must be kept in mind that these are the same criticisms that are levelled against the Israeli military and its role or the lack of it, in cyber security.[150]

---

[150] Many of these criticisms are summarised in the concluding chapter of Charles D. Freilich *et al, Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power,* (online edn.), Oxford Academic, 22 June 2023, p.197.

Appendix-1

Major Cyber incidents carried out by or against government and military targets

United States

The United States military has been both the target of cyber attacks as well as a perpetrator. While the former has received much publicity, there is much less information available on the latter. However, the Snowden Revelations hinted at the involvement of intelligence agencies in cyber espionage and hacking operations. The dual hatted nature of Cyber Command and the National Security Agency obscures the exact nature of these operations. More recently, the setting-up of hunt forward teams has been under the aegis of the US military. Despite efforts at creating a cyber-secure environment, both US military and government networks have been repeatedly penetrated, with the attackers mainly from China, Russia, Iran, North Korea, and East European countries. U.S. military doctrines have called for a response across the spectrum including kinetic responses to cyber attacks in furtherance of a policy of cyber deterrence. Other measures that have been taken include imposing sanctions on specific individuals.

The attacks listings have been classified under the categories of cyber-espionage, attacks on networks and phishing attempts. Reported attacks by US agencies are also included.

Cyber-espionage

- 2005. Chinese hackers infiltrated U.S. Department of Defense networks in an operation known as "Titan Rain." They targeted U.S. defense contractors, Army Information Systems Engineering Command; the Defense Information Systems

Agency; the Naval Ocean Systems Center; and the U.S. Army Space and Strategic Defense installation. (https://time.com/archive/6674509/the-invasion-of-the-chinese-cyberspies/)

- April 2005. Chinese hackers infiltrated NASA networks managed by Lockheed Martin and Boeing and exfiltrated information about the Space Shuttle Discovery program. (https://www.bloomberg.com/news/articles/2008-11-19/network-security-breaches-plague-nasa)

- 2007. Chinese hackers breached the Pentagon's Joint Strike Fighter project and stole data related to the F-35 fighter jet (https://www.theguardian.com/world/2009/apr/21/hackers-us-fighter-jet-strike)

- November 2008. Chinese hackers infiltrated the computer network of the White House and obtained emails between senior government officials (https://www.ft.com/content/2931c542-ac35-11dd-bf71-000077b07658)

- March 2009. Reports in the press say that the plans for Marine Corps 1, the new presidential helicopter, were found on a file-sharing network in Iran. (https://www.cbsnews.com/news/report-iran-stole-marine-one-specs-28-02-2009/)

- June 2009. The John Hopkins University's Applied Physics Laboratory, which does classified research for the Department of Defense and NASA, took its unclassified networks offline after they were penetrated. (https://thedailyrecord.com/2009/06/17/hopkins-applied-physics-lab-web-site-attacked)

- December 2009. Downlinks from U.S military UAVs were hacked by Iraqi insurgents using laptops and $24.99 file sharing software, allowing them to see what the UAV had viewed. (https://www.theguardian.com/world/2009/dec/17/skygrabber-american-drones-hacked)

- 2010. The PLA infiltrated the computer network of a Civilian Reserve Air Fleet (CRAF) contractor in which documents, flight details, credentials and passwords for encrypted email were stolen (https://www.armed-services.senate.gov/press-releases/sasc-

investigation-finds-chinese-intrusions-into-key-defense-contractors)

- April 2011. Employees at Oak Ridge National Laboratory received bogus emails with malware attachments. Two machines were infected and "a few megabytes" of data were extracted before the Lab was able to cut its internet connection. Oak Ridge was the target of an intrusion in 2007. (https://thehackernews.com/2011/04/oak-ridge-national-laboratory-hacked.html)

- July 2011. In a speech unveiling the Department of Defense's cyber strategy, the Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the DOD were stolen. (https://www.nbcnews.com/id/wbna43757768)

- October 2011. Networks of 48 companies in the chemical, defense, and other industries were penetrated for at least six months by a hacker looking for intellectual property. Some of the attacks are attributed to computers in Hebei, China. (https://www.nbcnews.com/id/wbna45105397)

- November 2011. According to a major U.S. news source, Chinese hackers interfered with two satellites belonging to NASA and USGS. (https://www.space.com/13423-hackers-government-satellites.html)

- February 2012. Media reports say that Chinese hackers stole classified information about the technologies onboard F-35 Joint Strike Fighters. (https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf)

- March 2012. Trend Micro uncovered a Chinese cyber campaign, dubbed 'Luckycat' that targeted U.S.-based activists and organizations, Indian and Japanese military research, as well as Tibetan activists (https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/luckycat-redux-campaign-attacks-multiple-targets-in-india-and-japan)

- March 2012. NASA's Inspector General reported that 13 APT attacks successfully compromised NASA computers in 2011. In

one attack, intruders stole 150 user credentials that could be used to gain unauthorized access to NASA systems. Another attack at the Joint Propulsion Laboratory involving China-based IP let the intruders gain full access to key JPL systems and sensitive user accounts. (https://www.wired.com/2012/03/jet-propulsion-lab-hacked)

- January 2013. A Defense Science Board report found that Chinese hackers stole U.S. weapons systems designs including for the PAC-3, THAAD, Aegis, F/A-18 fighter jet, V-22 Osprey, Black Hawk, and Littoral Combat Ship (https://www.bbc.com/news/world-us-canada-22692778)

- March 2013. Beginning in 2012, Chinese hackers targeted civilian and military maritime operations within the South China Sea, in addition to U.S. companies involved in maritime satellite systems, aerospace companies and defense contractors (https://therecord.media/china-linked-hackers-target-organizations-operating-in-south-china-sea)

- June 2013. PLA hackers infiltrated the computer networks of the U.S. Transportation Command and stole sensitive military information (https://www.theregister.com/2014/09/18/china_hacked_us_army_twenty_times_in_one_year/)

- September 2013. Chinese hackers used malware, known as 'Sykipot', to target entities in the U.S. Defense Industries and companies in key industries such as: telecommunications, computer hardware, government contractors, and aerospace. In mid-2013 they targeted the U.S. civil aviation sector (https://www.darkreading.com/vulnerabilities-threats/sykipot-malware-now-targeting-civil-aviation-information)

- July 2014. U.S. Office of Personnel Management networks that contain information on thousands of applicants for top secret clearances are breached. (https://www.bbc.com/news/world-us-canada-33017310)

- October 2014. A five-year cyber espionage campaign attributed to Russia exploits a zero-day vulnerability in Windows software on computers used by NATO, the EU and the Ukrainian

government. (https://www.bloomberg.com/news/articles/2014-10-14/russian-hackers-tracking-ukraine-crisis-stole-nato-data)

- November 2015. Dutch security firm Fox-IT identified a Chinese threat actor, 'Mofang', that had launched cyber attacks against government civilian and military agencies in the United States and other industries, including corporations conducting solar cell research (https://www.wired.com/2016/06/revealed-yet-another-chinese-group-hacking-countrys-economic-bottom-line)

- February 2017. An Iranian hacker group targeted actors associated with the U.S. defense industrial base as well as at least one human rights activist in a campaign to steal credentials and other data (https://iranprimer.usip.org/blog/2024/apr/24/us-sanctions-iranians-linked-cyberattacks)

- September 2017. Russia compromised the personal smartphones of NATO soldiers deployed to Poland and the Baltic states. (https://www.vox.com/world/2017/10/4/16424602/nato-russia-smartphone-hacking-report)

- October 2017. Reports surface that Russian government-backed hackers stole NSA hacking secrets from a contractor in 2015 by exploiting the Kaspersky antivirus software on the contractor's home computer (https://www.reuters.com/article/world/russian-hackers-stole-us-cyber-secrets-from-nsa-media-reports-idUSKBN1CA2DV)

- January 2018. Chinese hackers infiltrated a U.S. Navy contractor working for the Naval Undersea Warfare Center. 614 gigabytes of material related to a supersonic anti-ship missile for use on U.S. submarines were taken, along with submarine radio room information related to cryptographic systems and the Navy submarine development unit's electronic warfare library (https://www.nytimes.com/2018/06/08/us/politics/china-hack-navy-contractor-.html)

- April 2018. A cyber espionage campaign originating in China collected data from satellite, telecom, and defense organizations

in the United States and Southeast Asia (https://www.courthousenews.com/feds-charge-chinese-spies-with-hacking-us-aerospace-firms)

- November 2018. Security researchers report that Russian hackers impersonating U.S. State Department officials attempted to gain access to the computer systems of military and law enforcement agencies, defense contractors, and media companies. (https://www.securityweek.com/suspected-russian-hackers-impersonate-state-department-aide/)

- December 2018. U.S. Navy officials report that Chinese hackers had repeatedly stolen information from Navy contractors including ship maintenance data and missile plans.(https://www.bbc.com/news/technology-47468443)

- March 2019. Chinese hackers targeted Israeli defense firms that had connections to the U.S. military (https://www.voanews.com/a/east-asia-pacific_chinese-hackers-used-cyber-disguising-technology-against-israel-report-finds/6209720.html)

- April 2019. Chinese hackers stole General Electric's trade secrets concerning jet engine turbine technologies (https://www.justice.gov/opa/pr/former-ge-power-engineer-convicted-conspiracy-commit-economic-espionage)

- May 2019. Hackers affiliated with the Chinese intelligence service reportedly had been using NSA hacking tools since 2016, more than a year before those tools were publicly leaked. (https://edition.cnn.com/2019/05/07/politics/china-nsa-hacking/index.html)

- December 2019. Microsoft won a legal battle to take control of 50 web domains used by a North Korean hacking group to target government employees, think tank experts, university staff, and others involved in nuclear proliferation issues (https://blogs.microsoft.com/on-the-issues/2019/12/30/microsoft-court-action-against-nation-state-cybercrime)

- August 2020. Hackers for hire suspected of operating on behalf of the Iranian government were found to have been working to gain access to sensitive information held by North American and Israeli entities across a range of sectors, including technology, government, defense, and healthcare. (https://www.theverge.com/2024/4/24/24139160/doj-iranian-nationals-cyberattack-charge)

- September 2020. Three hackers operating at the direction of Iran's Islamic Revolutionary Guard Corps were indicted by the United States for attacks against workers at aerospace and satellite technology companies, as well as international government organizations. (https://iranprimer.usip.org/blog/2024/apr/24/us-sanctions-iranians-linked-cyberattacks)

- October 2020. The NSA warned that Chinese government hackers were targeting the U.S. defense industrial base as part of a wide-ranging espionage campaign (https://www.foxbusiness.com/technology/nsa-advisory-warns-defense-department-about-chinese-government-hackers)

- October 2020. The FBI, CISA and U.S. Cyber Command announced that a North Korean hacking group had been conducting a cyber espionage campaign against individual experts, think tanks, and government entities in South Korea, Japan, and the United States with the purpose of collecting intelligence on national security issues related to the Korean peninsula, sanctions, and nuclear policy

- October 2020. A spokesperson for China's Foreign Ministry responded to accusations that Chinese state-sponsored hackers were targeting the U.S. defense industrial base by declaring that the United States was an "empire of hacking," citing 2013 leaks about the NSA's Prism program. (http://gb.china-embassy.gov.cn/eng/PressandMedia/Spokepersons/202305/P020230508664391507653.pdf)

- December 2020. Over 200 organizations around the world—including multiple US government agencies—were revealed to have been breached by Russian hackers who compromised the

software provider SolarWinds and exploited their access to monitor internal operations and exfiltrate data. (https://www.govtech.com/security/list-of-hacked-organizations-tops-200-in-solarwinds-case.html)

- March 2021. Chinese government hackers targeted Microsoft's enterprise email software to steal data from over 30,000 organizations around the world, including government agencies, legislative bodies, law firms, defense contractors, infectious disease researchers, and policy think tanks. (https://www.nytimes.com/2023/07/11/us/politics/china-hack-us-government-microsoft.html)

- April 2021. Two state-backed hacking groups—one of which works on behalf of the Chinese government—exploited vulnerabilities in a VPN service to target organizations across the U.S. and Europe with a particular focus on U.S. defense contractors. (https://www.reuters.com/technology/china-linked-hackers-used-pulse-secure-flaw-target-us-defense-industry-2021-04-20)

- December 2021. Chinese hackers breached four more U.S. defense and technology firms in December, in addition to one organization in November. The hackers obtained passwords to gain access to the organizations' systems and looked to intercept sensitive communications. (https://therecord.media/chinese-hackers-behind-guam-hack-targeting-us-for-years)

- February 2022. Russian state-sponsored actors hacked into numerous U.S. defense contractors between January 2020 and February 2022. The hackers exfiltrated emails and sensitive data relating to the companies' export-controlled products and proprietary information and interactions with foreign governments. (https://www.axios.com/2022/02/16/us-intelligence-russia-hacker-defense-contractors)

Network attack

- September 2007. Contractors employed by DHS and DOD had their networks hacked as backdoors into agency systems.

(https://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471_pf.html)

- September 2011. A computer virus from an unknown source introduced "keylogger" malware onto ground control stations for US Air Force UAVs and, according to press reports, infected both classified and unclassified networks at Creech Air Force Base in Nevada. The US did not lose control of any drone, nor does it appear that any data was exfiltrated, but the malware was persistent and took several attempts to remove. (https://phys.org/news/2011-10-virus-drone-fleet.html)

- October 2014. The Department of State reports breaches of its unclassified networks and shut down its entire unclassified email system to repair possible damage. A month later, "suspicious cyber activity" was noticed on a White House computer network, but the White House said that no classified networks had been breached. (https://edition.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/index.html)

- October 2014. The National Oceanic and Atmospheric Administration (NOAA) at the U.S. Department of Commerce is hacked, skewing the accuracy of some National Weather Service forecasts, according to NOAA. (https://www.dispatch.com/story/business/information-technology/2014/11/16/china-hacked-into-national-weather/24040517007/)

- August 2016. A group calling itself "Shadow Brokers" claimed to have penetrated NSA and published a collection of NSA tools on Pastebin. (https://www.wired.com/story/nsa-hacking-tools-stolen-hackers/)

- October 2018. The U.S. Department of Justice indicted Chinese intelligence officers and hackers working for them for engaging in a campaign to hack into U.S. aerospace companies and steal information (https://cyberscoop.com/doj-unseals-charges-against-10-chinese-nationals-for-hacking-aerospace-companies).

- July 2019. U.S. Cybercommand issued an alert warning that government networks were being targeted with malware associated with a known Iran-linked hacking group(https://cyberscoop.com/u-s-cyber-command-iranian-hacking-malware-virustotal)

- July 2019. The U.S. Coast Guard issued a warning after it received a report that a merchant vessel had its networks disrupted by malware while traveling through international waters (https://www.ajot.com/insights/full/ai-u.s-coast-guard-warns-of-cyber-attack-electronic-interference-threats-to-commercial-vessels)

- March 2021. Suspected Russian hackers stole thousands of emails after breaching the email server of the U.S. State Department. (https://www.politico.com/news/2021/03/30/russia-suspected-emails-478541)

- November 2021. Hackers gained access to the social security and driver's license numbers of employees after compromising a U.S. defense contractor (https://www.securityweek.com/us-government-contractor-ewa-discloses-data-theft-breach)

- October 2020. The U.S. Department of Homeland Security revealed that hackers targeted the U.S. Census Bureau in a possible attempt to collect bulk data, alter registration information, compromise census infrastructure, or conduct DoS attacks (https://fortune.com/2021/08/18/us-census-bureau-hit-by-cyber-attack-2020/)

Phishing

- March-April 2011. Hackers used phishing techniques in an attempt to obtain data that would compromise RSA's SecureID authentication technology. The data acquired was then used in an attempt to penetrate Lockheed Martin's networks (https://www.theregister.com/2011/04/04/rsa_hack_howdunnit/)

- May 2014. Alleged Chinese hackers posed as C-Suite executives in a spear phishing campaign to access the network of Alcoa. The hackers stole 2,907 emails and 863 attachments. (https://

www.wsj.com/articles/alleged-chinese-hacking-alcoa-breach-relied-on-simple-phishing-scam-1400543823)

- July 2015. A spear phishing attack on the Joint Chiefs of Staff unclassified email servers resulted in the system being shut down for 11 days while cyber experts rebuilt the network, affecting the work of roughly 4,000 military and civilian personnel. Officials believe that Russia is responsible for the intrusion, which occurred sometime around July 25, although China has not been ruled out as the perpetrator. (https://www.usatoday.com/story/news/nation/2015/08/06/russia-reportedly-hacks-pentagon-email-system/31228625/)

- March 2017. An intelligence report revealed a Russian operation to send malicious spear-phishing messages to more than 10,000 Twitter users in the Department of Defense. The malicious payloads delivered through these messages gave Russian hackers access to the victim's device and Twitter account. (https://www.theverge.com/2017/5/18/15658300/russia-hacking-twitter-bots-pentagon-putin-election)

- April 2017. The Lazarus Group, thought to be associated with North Korea, was found to be involved in a spear phishing campaign against US defense contractors (https://cyberscoop.com/lazarus-group-north-korea-us-defense-contractors)

- June 2020. Suspected North Korean hackers compromised at least two defense firms in Central Europe by sending false job offers to their employees while posing as representatives from major U.S. defense contractors (https://cyberscoop.com/north-korea-aerospace-defense-mcafee-job-offers/)

- July 2021. Iran used Facebook accounts to pose as recruiters, journalists, and NGO affiliates, targeting U.S. military personnel. The hackers sent malware-infected files or tricked targets into submitting sensitive credentials to phishing sites. (https://therecord.media/facebook-disrupts-iranian-group-targeting-us-defense-and-aerospace-sectors)

- November 2021. Hackers gained access to the FBI's Law Enforcement Enterprise Portal—a system used to communicate to state and local officials—and sent a warning of a cyberattack in an email claiming to be from the Department of Homeland Security (DHS). (https://www.washingtonpost.com/nation/2021/11/14/fbi-hack-email-cyberattack/

Attacks by US entities much of these is taken from Edwards Snowdens revelations. Only those that could be corroborated are added here

- October 2007. China's Ministry of State Security said that foreign hackers, 42% from Taiwan and 25% from the United Sates, had been stealing information from Chinese key areas. In 2006, when China's China Aerospace Science & Industry Corporation (CASIC) Intranet Network was surveyed, spywares were found in the computers of classified departments and corporate leaders.

- June 2013. Edward Snowden, a former systems administrator at the NSA, reveals documents showing among other things that the US conducted cyber espionage against Chinese targets. (https://blokt.com/guides/edward-snowden-leaks)

- September 2013. The U.S. Navy says that Iran hacked into unclassified networks. (https://www.theverge.com/2014/2/18/5421636/us-navy-hack-by-iran-lasted-for-four-months-say-officials)

- October 2010. Stuxnet, a complex piece of malware designed to interfere with Siemens Industrial Control Systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear program. (https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html)

- October 2013. Press reports based on Snowden leaks reveal NSA hacked into German Chancellor Merkel's mobile phone, one of a larger series of leaks on NSA activities.(https://www.theguardian.com/world/2015/jun/12/germany-drops-inquiry-into-claims-nsa-tapped-angela-merkels-phone)

- June 2015. Media reports say that Stuxnet-like attacks were attempted against North Korea by the U.S., without success. (https://www.wired.com/2015/05/us-tried-stuxnet-north-koreas-nuclear-program)

- July 2015. A spear phishing attack on the Joint Chiefs of Staff unclassified email servers resulted in the system being shut down for 11 days while cyber experts rebuilt the network, affecting the work of roughly 4,000 military and civilian personnel. Officials believe that Russia is responsible for the intrusion, which occurred sometime around July 25, although China has not been ruled out as the perpetrator. (https://edition.cnn.com/2015/08/05/politics/joint-staff-email-hack-vulnerability/index.html)

- March 2017. Wikileaks released a trove of sophisticated CIA hacking tools dated from 2013 to 2016, claiming that the release reflected several hundred million lines of CIA-developed code. (https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html)

- October 2017. Russian hackers reported to be targeting potential attendees of CyCon, a cybersecurity conference organized by the US Army and the NATO CCD COE (https://executivegov.com/2017/10/foreign-hacking-group-targets-cybersecurity-conference-attendees-with-phishing-campaign/)

- October 2018. U.S. defense officials announced that Cyber Command had begun targeting individual Russian operatives to deter them from interfering in the 2018 midterm elections. (https://www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html)

- October 2018. The head of Iran's civil defense agency announced that the country had recently neutralized a new, more sophisticated version of Stuxnet (https://www.bbc.com/news/world-middle-east-20842113)

- June 2019. The U.S. announced it had launched offensive cyber operations against Iranian computer systems used to control

missile and rocket launches. (https://www.vox.com/2019/6/23/18714327/iran-us-donald-trump-cyberattack-drone-strike)

- June 2019. Iran announced that it had exposed and helped dismantle an alleged CIA-backed cyber espionage network across multiple countries (https://www.scmagazine.com/news/report-iran-claims-to-have-thwarted-a-u-s-cyber-espionage-operation)

- September 2019. Huawei accused the U.S. government of hacking into its intranet and internal information systems to disrupt its business operations. (https://www.latimes.com/business/technology/story/2019-09-04/huawei-us-cyber-attacks-coercing-employees)

- July 2020. Media reports say a 2018 Presidential finding authorized the CIA to conduct cyber operations against Iran, North Korea, Russia, and China. The operations included disruption and public leaking of information. (https://www.yahoo.com/news/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html)

- July 2020. President Trump confirmed that he directly authorized a 2019 operation by US Cyber Command taking the Russian Internet Research Agency offline. (https://edition.cnn.com/2020/07/10/politics/donald-trump-us-russia-cyberattack/index.html)

- November 2020. U.S. Cyber Command and the NSA conducted offensive cyber operations against Iran to prevent interference in the upcoming U.S. elections. (https://www.cbsnews.com/news/election-interference-us-cyber-command-nsa-nakasone/)

- February 2022. A Beijing-based cybersecurity company accused the U.S. National Security Agency of engineering a back-door to monitor companies and governments in over 45 countries around the world. A Foreign Ministry spokesman said that operations like this may threaten the security of China's critical infrastructure and compromise trade secrets. (https://www.itnews.com.au/news/chinese-researchers-attribute-top-tier-backdoor-to-nsa-equation-group-576528)

Russia

While must much of the cyber attacks traced to Russia are perceived to be carried out by cyber criminals, a perusal of these attacks shows that many targeted towards military and government networks of countries both friendly and hostile to Russia. With cyber largely the domain of the intelligence agencies, it is evident that there are many non state actors working under the command and control of these agencies. The need for plausible deniability has resulted in very loose control over these hackers. It is also doubtful whether the data collected has been put to optimum use since that would require the creation of downstream entities for data analysis. It also remains to be seen how long the Russian structure of cyber operations can remain viable. Much as the Wagner group had to be dismantled, its cyber entity, the Internet Research Agency, also had to be dismantled after it turned on the Russian authorities and began to disseminate disinformation against the Putin administration.

Cyber-espionage

Attacks by Russia

- May 2006. The Department of State's networks were hacked, and unknown foreign intruders downloaded terabytes of information. https://www.cbsnews.com/news/state-department-computers-hacked/

- October 2012. A Russian cybersecurity firm found a virus used against embassies, research firms, military installations, energy providers, and critical infrastructure in Eastern Europe, Russia, and Central Asia. https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-identifies-operation—red-october—an-advanced-cyber-espionage-campaign-targeting-diplomatic-and-government-institutions-worldwide

- October 2014. A five-year cyber espionage campaign attributed to Russia exploits a zero-day vulnerability in Windows software on computers used by NATO, the EU and the Ukrainian

government. https://www.dw.com/en/russian-hackers-stole-us-secrets-from-nsa/a-40827823

- April 2017. The Danish Defense Intelligence Service reported that a "foreign player," alleged by the Danish press to be Russia espionage group, had accessed Defense Ministry email accounts in 2015 and in 2016, but was unable to retrieve classified information. https://www.atlanticcouncil.org/blogs/natosource/denmark-russia-hacked-our-defense-ministry-for-two-years/

- October 2017. Reports surface that Russian government-backed hackers stole NSA hacking secrets from a contractor in 2015 by exploiting the Kaspersky antivirus software on the contractor's home computer https://thehackernews.com/2017/10/kaspersky-nsa-spying.html

- October 2017. A major wave of ransomware infections hits media organizations, train stations, airports, and government agencies in Russia and Eastern Europe. Security researchers found strong evidence linking the attack to the creators of NotPetya, and noted that the malware used leaked NSA-linked exploits to move through networks. Ukrainian police later reported that the ransomware was a cover for a quiet phishing campaign undertaken by the same actor to gain remote access to financial and other confidential data. https://www.cisa.gov/news-events/alerts/2017/10/24/multiple-ransomware-infections-reported

- October 2017. Russian hackers reported to be targeting potential attendees of CyCon, a cybersecurity conference organized by the US Army and the NATO CCD COE https://cyberscoop.com/fancy-bear-cycon-spear-phishing-cisco-talos

- February 2018. German news reported that a Russian hacking group had breached the online networks of Germany's foreign and interior ministries, exfiltrating at least 17 gigabytes of data in an intrusion that went undetected for a year. https://www.c4isrnet.com/international/2018/02/28/report-russian-group-hacked-german-government-network

- June 2018. The U.S. Treasury Department announced sanctions against five Russian companies and three individuals for enabling Russian intelligence and military units to conduct cyberattacks against the U.S. https://home.treasury.gov/news/press-releases/sm0410

- October 2018. The U.S. Justice Department announces criminal charges against seven GRU officers for multiple instances of hacking against organizations including FIFA, Westinghouse Electric Company, the Organisation for the Prohibition of Chemical Weapons, and the U.S. and World Anti-Doping Agencies. https://edition.cnn.com/2018/10/04/politics/justice-department-russian-intelligence-officers/index.html

- October 2018. U.S. agencies warned President Trump that China and Russia eavesdropped on calls he made from an unsecured phone. https://www.nytimes.com/2018/10/24/us/politics/trump-phone-security.html

- December 2018. The Czech security service announced that Russian intelligence services were discovered to have been behind attacks against the Czech foreign ministry in 2017 https://www.zdnet.com/article/czech-republic-blames-russia-for-multiple-government-network-hacks/

- January 2019. France attributed a cyberattack targeting the Ministry of Defense to a Russian based hacking group. The attack targeted the mailboxes of nineteen executives of the ministry.

- August 2019. The Czech Republic announced that the country's Foreign Ministry had been the victim of a cyberattack by an unspecified foreign state, later identified as Russia

- October 2019. A state-sponsored hacking group targeted diplomats and high-profile Russian speaking users in Eastern Europe. https://www.securityweek.com/czechs-blame-foreign-state-foreign-ministry-cyberattack

- April 2020. Poland suggested the Russian government was being behind a series of cyber attacks on Poland's War Studies University meant to advance a disinformation campaign undermining U.S.-

Polish relations. https://medium.com/dfrlab/cyber-based-disinformation-operation-targets-u-s-poland-alliance-a7033a83700

- August 2020. Russian hackers compromised news sites and replaced legitimate articles with falsified posts that used fabricated quotes from military and political officials to discredit NATO among Polish, Lithuanian, and Latvian audiences https://securityaffairs.com/163080/cyber-crime/russian-hackers-british-newspaper-websites.html

- September 2021. The EU formally blamed Russia for its involvement in the 'Ghostwriter' cybercampaign, which targeted the elections and political systems of several member states. Since 2017, Russian operators hacked the social media accounts of government officials and news websites, with the goal of creating distrust in U.S. and NATO forces. https://therecord.media/eu-formally-blames-russia-for-ghostwriter-hack-and-influence-operation

- February 2022. Russian state-sponsored actors hacked into numerous U.S. defense contractors between January 2020 and February 2022. The hackers exfiltrated emails and sensitive data relating to the companies' export-controlled products and proprietary information and interactions with foreign governments. https://hivepro.com/threat-advisory/russian-state-sponsored-cyber-actors-targeting-u-s-critical-infrastructure

Attacks against Russia

- October 2020. A North Korean hacker group carried out attacks against aerospace and defense companies in Russia https://www.ewdn.com/2020/10/20/north-korean-hacker-group-attacked-aerospace-and-defense-targets-in-russia

- May 2021. A Chinese hacking group compromised a Russian defense contractor involved in designing nuclear submarines for the Russian navy. https://therecord.media/china-linked-apt-group-targets-russian-nuclear-sub-designer-with-an-undocumented-backdoor

- July 2021. The Russian defense ministry claimed it was hit with a DDoS attack that caused its website to shut down, stating the attack came from outside the Russian Federation. https://tass.com/defense/1314641

- January 2022. A DRPK-affiliated group targeted multiple Russian diplomats with malware. The diplomats received an email disguised as a New Year greetings screensaver but which, after being opened, installed a remote access trojan. https://thehackernews.com/2022/01/north-korean-hackers-start-new-year.html

Network Attack

Attacks by Russia

- April 2015. The Pentagon revealed that Russian hackers gained access to an unclassified network within the DOD, though Pentagon officials were able to block the hackers' access within 24 hours. https://www.theguardian.com/technology/2015/aug/06/us-military-joint-chiefs-hacked-officials-blame-russia

- July 2018. Ukrainian intelligence officials claim to have thwarted a Russian attack on the network equipment of a chlorine plant in central Ukraine. The virus used in the attack is the same malware responsible for the infection of 500,000 routers worldwide in a campaign the FBI linked to state sponsored Russian hackers. https://cyware.com/news/ukraine-says-it-stopped-russian-vpnfilter-malware-attack-on-a-chlorine-distillation-plant-4f379f78

- November 2018. Security researchers report that Russia launched coordinated cyber attacks against Ukrainian government and military targets before and during the attack on Ukrainian ships in late November https://www.cgai.ca/russian_cyber_operations_in_ukraine_and_the_implications_for_nato

- June 2021. Hackers working on behalf of Russian intelligence services are believed to have hacked Netherlands police internal network in 2017. The attack occurred during the country's

investigation of the Malaysia Airlines Flight 17 (MH17) that was shot down in 2014. https://securityaffairs.com/118794/apt/russia-linked-apt-dutch-police.html

Phishing

Attack by Russia

- July 2015. A spear phishing attack on the Joint Chiefs of Staff unclassified email servers resulted in the system being shut down for 11 days while cyber experts rebuilt the network, affecting the work of roughly 4,000 military and civilian personnel. Officials believe that Russia is responsible for the intrusion, which occurred sometime around July 25, although China has not been ruled out as the perpetrator. https://www.theguardian.com/technology/2015/aug/06/us-military-joint-chiefs-hacked-officials-blame-russia

- March 2017. An intelligence report revealed a Russian operation to send malicious spear-phishing messages to more than 10,000 Twitter users in the Department of Defense. The malicious payloads delivered through these messages gave Russian hackers access to the victim's device and Twitter account. https://www.yahoo.com/news/russian-hackers-accused-targeting-u-153343277.html

- June 2017. A Russia-linked hacking group was found to have launched a spear-phishing campaign against Montenegro after the country announced its decision to join NATO https://www.securityweek.com/russian-hackers-target-montenegro-country-joins-nato/

- November 2018. Security researchers report that Russian hackers impersonating U.S. State Department officials attempted to gain access to the computer systems of military and law enforcement agencies, defense contractors, and media companies https://www.reuters.com/article/world/russians-impersonating-us-state-department-aide-in-hacking-campaign-research-idUSKCN1NL2B6/

- November 2019. A Russian-speaking hacking group targeted a wide range of Kazakh individuals and organisations including government agencies, military personnel, foreign diplomats, journalists, dissidents, and others through a combination of spear phishing and physical device compromise. https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan

- December 2019. Russian government hackers targeted Ukrainian diplomats, government officials, military officers, law enforcement, journalists, and nongovernmental organizations in a spear phishing campaign https://www.npr.org/2024/05/30/nx-s1-4984993/russia-linked-hackers-phishing-campaign-against-ukraine-is-disrupted

- September 2020. Russian hackers targeted government agencies in NATO member countries, and nations who cooperate with NATO. The campaign uses NATO training material as bait for a phishing scheme that infects target computers with malware that creates a persistent backdoor https://www.reuters.com/world/europe/russian-hackers-targeted-nato-eastern-european-militaries-google-2022-03-30/

Ransomware

- June 2017. Russian hackers used an updated ransomware program to target Ukrainian infrastructure, including power companies, airports, and public transit. https://economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-cyberattack-that-shook-the-world/articleshow/89997076.cms

- June 2017. A NotPetya ransomware attack shut down the port terminals of Danish shipping giant Maersk for two days, causing an estimated $300 million in associated costs https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

- May 2021. On May 6, the Colonial Pipeline, the largest fuel pipeline in the United States, was the target of a ransomware

attack. The energy company shut down the pipeline and later paid a $5 million ransom. The attack is attributed to DarkSide, a Russian speaking hacking group. https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html

- May 2021. On May 14, Ireland's national health service, the Health Service Executive (HSE), was the victim of a ransomware attack. Upon discovering the attack, government authorities shut down the HSE system. The attackers utilized the Conti ransomware-as-a-service (RaaS), which is reported to be operated by a Russia-based cybercrime group. https://www.bbc.com/news/world-europe-57111615

- May 2021. The world's largest meat processing company, Brazilian-based JBS, was the victim of a ransomware attack. The attack shut down facilities in the United States, Canada and Australia. The attack was attributed to the Russian speaking cybercrime group, REvil. https://www.vox.com/recode/2021/6/1/22463179/jbs-foods-ransomware-attack-meat-hackers

- July 2021. Russian hackers exploited a vulnerability in Kaseya's virtual systems/server administrator (VSA) software allowing them to deploy a ransomware attack on the network. The hack affected around 1,500 small and midsized businesses, with attackers asking for $70 million in payment. https://edition.cnn.com/2021/07/06/tech/kaseya-ransomware-what-we-know/index.html

- December 2021. A Russian group took responsibility for a ransomware attack on Australian utility company CS energy. This announcement came after Australian media outlets blamed Chinese government hackers for the attack. https://www.securityweek.com/australian-electricity-provider-cs-energy-hit-ransomware/

- February 2022. Multiple oil terminals in some of Europe's biggest ports across Belgium and Germany fell victim to a cyberattack, rendering them unable to process incoming barges. A ransomware strain associated with a Russian-speaking hacking

group was used to disrupt the ability of energy companies to process payments. https://www.euronews.com/2022/02/03/oil-terminals-disrupted-after-european-ports-hit-by-cyberattack

List of major cyber incidents-China

Chinese cyber attacks have largely been under the aegis of the military even though China has not acknowledged that the PLA has offensive cyber operations capability. Cyber espionage on Western companies was the focus for many years. Subsequently, the focus expanded to include data exfiltration, especially, from government entities around the world. China has also carried out disruptive and destructive attacks against many countries though accusations are always met with counter accusations.

Cyber-espionage

Attacks by China

- 2005. Chinese hackers infiltrated U.S. Department of Defense networks in an operation known as "Titan Rain." They targeted U.S. defense contractors, Army Information Systems Engineering Command; the Defense Information Systems Agency; the Naval Ocean Systems Center; and the U.S. Army Space and Strategic Defense installation https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1100/RRA1190-1/RAND_RRA1190-1.pdf

- April 2005. Chinese hackers infiltrated NASA networks managed by Lockheed Martin and Boeing and exfiltrated information about the Space Shuttle Discovery program https://www.nbcnews.com/news/investigations/chinese-hackers-stole-boeing-lockheed-military-plane-secrets-feds-n153951

- August 2006. Chinese hackers found targeting the U.S. Department of Defense, scanning networks and downloading terabytes of data, posing a significant threat. https://www.computerworld.com/article/1520816/china-s-hackers-at-war-with-pentagon-systems.html

- 2007. Chinese hackers breached the Pentagon's Joint Strike Fighter project and stole data related to the F-35 fighter jet https://

www.theguardian.com/world/2009/apr/21/hackers-us-fighter-jet-strike

- January 2010. M. K. Narayanan, India's National Security Adviser, said his office and other government departments were attacked by China on December 15. The Prime Minister's office later denied that their computers had been hacked. Narayanan said this was not the first attempt to penetrate Indian government computers. https://www.indiatoday.in/latest-headlines/story/chinese-hackers-target-pmo-65017-2010-01-13

- March 2010. Australian authorities said there were more than 200 attempts to hack into the networks of the legal defense team for Rio Tinto executives being tried in China to gain inside information on the trial defense strategy https://www.bloomberg.com/news/features/2018-07-13/did-china-hack-rio-tinto-to-gain-a-billion-dollar-advantage

- April 2010. Chinese hackers reportedly broke into classified files at the Indian Defence Ministry and Indian embassies around the world, gaining access to Indian missile and armament systems. https://timesofindia.indiatimes.com/india/chinese-agents-hack-into-indias-secret-documents-report/articleshow/5766129.cms

- October 2011. Networks of 48 companies in the chemical, defense, and other industries were penetrated for at least six months by a hacker looking for intellectual property. Some of the attacks are attributed to computers in Hebei, China https://www.theguardian.com/technology/2011/nov/01/china-hacking-chemical-military-companies

- February 2012. Media reports say that Chinese hackers stole classified information about the technologies onboard F-35 Joint Strike Fighters. https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/

- March 2012. Trend Micro uncovered a Chinese cyber campaign, dubbed 'Luckycat' that targeted U.S.-based activists and organizations, Indian and Japanese military research, as well as Tibetan activists https://www.indiatoday.in/world/americas/story/chinese-hackers-attack-indian-websites-97678-2012-03-30

- July 2012. Indian naval officials confirmed that a virus had collected data from sensitive computer systems at the country's Eastern Naval Command headquarters and sent the data to Chinese IP addresses. The virus allegedly entered the Navy's network via infected USB drives, which were used to transfer data from standalone computers holding sensitive files to networked systems. https://www.bbc.com/news/technology-18703508

- January 2013. A Defense Science Board report found that Chinese hackers stole U.S. weapons systems designs including for the PAC-3, THAAD, Aegis, F/A-18 fighter jet, V-22 Osprey, Black Hawk, and Littoral Combat Ship https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html

- March 2013. The Indian Defence Research and Development Organization (DRDO) was hacked, with thousands of documents uploaded to a server with an IP address in Guangdong, China https://www.newindianexpress.com/nation/2013/Mar/14/chinese-hack-drdo-computers-antony-seeks-report-458371.html

- March 2013. Hackers used a Chinese IP address to attack South Korean banks and broadcasters. https://www.bbc.com/news/world-asia-21873017

- May 2013. An alleged Chinese hacker steals the blueprints for the Australian Security Intelligence Organization's new $631 million building. https://www.reuters.com/article/world/australian-spy-hq-plans-stolen-by-chinese-hackers-report-idUSBRE94R02B/

- June 2013. PLA hackers infiltrated the computer networks of the U.S. Transportation Command and stole sensitive military information https://www.defenseone.com/technology/2014/09/china-hacks-us-military-transport-contractors/94445/

- September 2013. Chinese hackers used malware, known as 'Sykipot', to target entities in the U.S. Defense Industries and companies in key industries such as: telecommunications, computer hardware, government contractors, and aerospace. In mid-2013 they targeted the U.S. civil aviation sector. https://www.nbcnews.com/id/wbna45985897

- July 2014. Canada's Foreign Minister asks his Chinese counterpart about PLA cyber espionage against the National Research Council, Canada' leading technology research agency. https://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241

- May 2015. Chinese intelligence officers infiltrated networks and exfiltrated trade secret information about turbofan engines from U.S. and European aerospace firms over the course of five years (https://www.washingtonpost.com/world/national-security/us-charges-chinese-spies-and-their-recruited-hackers-in-conspiracy-to-steal-trade-secrets/2018/10/30/50fadb94-dc82-11e8-b732-3c72cbf131f2_story.html)

- January 2018. Chinese hackers infiltrated a U.S. Navy contractor working for the Naval Undersea Warfare Center. 614 gigabytes of material related to a supersonic anti-ship missile for use on U.S. submarines were taken, along with submarine radio room information related to cryptographic systems and the Navy submarine development unit's electronic warfare library https://www.csoonline.com/article/565596/chinese-hackers-stole-614gb-of-undersea-warfare-data-from-us-navy-contractor.html

- April 2018. Reports from cyber security researchers indicate that Chinese state-sponsored hacking groups have targeted Japanese defense companies in an attempt to gain information on Tokyo's policies towards North Korea https://fortune.com/2018/04/23/china-japan-north-korea-cyberspies-secrets/

- October 2018. The U.S. Department of Justice indicted Chinese intelligence officers and hackers working for them for engaging in a campaign to hack into U.S. aerospace companies and steal information https://www.justice.gov/opa/pr/chinese-

intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal

- December 2018. U.S. Navy officials report that Chinese hackers had repeatedly stolen information from Navy contractors including ship maintenance data and missile plans. https://www.wsj.com/articles/u-s-navy-is-struggling-to-fend-off-chinese-hackers-officials-say-11544783401

- February 2019. European aerospace company Airbus reveals it was targeted by Chinese hackers who stole the personal and IT identification information of some of its European employees. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

- March 2019. Chinese hackers targeted Israeli defense firms that had connections to the U.S. military https://foreignpolicy.com/2019/03/24/china-and-russia-are-spying-on-israel-to-steal-u-s-secrets-putin-netanyahu-xi-haifa-ashdod-iai-elbit/

- April 2019. Chinese hackers stole General Electric's trade secrets concerning jet engine turbine technologies https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade

- May 2019. Hackers affiliated with the Chinese intelligence service reportedly had been using NSA hacking tools since 2016, more than a year before those tools were publicly leaked. https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html

- January 2020. Mitsubishi announces that a suspected Chinese group had targeted the company as part of a massive cyberattack that compromised personal data of 8,000 individuals as well as information relating to partnering businesses and government agencies, including projects relating to defense equipment. https://www.scmp.com/week-asia/economics/article/3046825/japans-mitsubishi-electric-targeted-cyberattack-blamed-chinese

- August 2020. Seven semiconductor vendors in Taiwan were the victim of a two-year espionage campaign by suspected Chinese

state hackers targeting firms' source code, software development kits, and chip designs. https://www.indiatoday.in/news-analysis/story/exposed-china-s-hacking-campaign-to-unsettle-taiwan-economy-1713259-2020-08-20

- March 2021. Chinese government hackers targeted Microsoft's enterprise email software to steal data from over 30,000 organizations around the world, including government agencies, legislative bodies, law firms, defense contractors, infectious disease researchers, and policy think tanks. https://www.reuters.com/article/idUSKCN2AU2MF/

- April 2021. Two state-backed hacking groups—one of which works on behalf of the Chinese government—exploited vulnerabilities in a VPN service to target organizations across the U.S. and Europe with a particular focus on U.S. defense contractors. https://www.reuters.com/technology/china-linked-hackers-used-pulse-secure-flaw-target-us-defense-industry-2021-04-20/

- May 2021. A Chinese hacking group compromised a Russian defense contractor involved in designing nuclear submarines for the Russian navy. https://thehackernews.com/2021/05/new-chinese-malware-targeted-russias.html

- December 2021. Chinese hackers breached four more U.S. defense and technology firms in December, in addition to one organization in November. The hackers obtained passwords to gain access to the organizations' systems and looked to intercept sensitive communications. https://edition.cnn.com/2021/12/02/politics/china-hackers-espionage-defense-contractors/index.html

- March 2022. Hackers linked to the Chinese government penetrated the networks belonging to government agencies of at least 6 different U.S. states in an espionage operation. Hackers took advantage of the Log4j vulnerability to access the networks, in addition to several other vulnerable internet-facing web

applications. https://www.theverge.com/2022/3/8/22966517/china-hack-government-networks-apt41-usaherd

- August 2022. A Chinese-speaking hacking group, TA428, targeted organizations in Eastern Europe and Afghanistan, using phishing emails and malware to infiltrate and control IT systems, exfiltrating sensitive data to servers in China. https://therecord.media/china-linked-group-targeted-government-agencies-defense-firms-in-eastern-europe

- May 2023. Chinese hackers installed malicious code in Guam's telecom systems, raising alarms due to its strategic military importance. https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html

- April 2024 A cyber-attack exposed 270,000 UK military payroll records, suspected to be by Chinese hackers, causing significant security concerns. https://www.theguardian.com/uk-news/article/2024/may/07/270000-uk-forces-records-thought-to-have-been-exposed-to-chinese-hackers

Attack Against China

- April 2009. Prime Minister Wen Jiabao announced that hacker from Taiwan accessed a Chinese State Council computer containing drafts of his report to the National People's Congress. https://www.scmp.com/article/675347/hackers-tap-wens-work-report

- June 2015. The Chinese company Qihoo360 reports discovering "OceanLotus," an espionage program operating since 2012 to target marine agencies, research institutions and shipping companies. https://www.darkreading.com/vulnerabilities-threats/chinese-isp-china-is-victim-of-foreign-state-backed-apt-group

- November 2018. Chinese state media reports that the country had been the victim of multiple attacks by foreign hackers in 2018, including the theft of confidential emails, utility design plans, lists of army units, and more

- March 2020. Chinese cybersecurity firm Qihoo 360 accused the CIA of being involved in an 11- year long hacking campaign against Chinese industry targets, scientific research organizations, and government agencies https://ciso.economictimes.indiatimes.com/news/cia-accused-of-11-year-long-cyber-espionage-against-china/74470194

- February 2022. A Beijing-based cybersecurity company accused the U.S. National Security Agency of engineering a backdoor to monitor companies and governments in over 45 countries around the world. A Foreign Ministry spokesman said that operations like this may threaten the security of China's critical infrastructure and compromise trade secrets. https://www.globaltimes.cn/page/202202/1252952.shtml

- March 2024. China's Ministry of State Security revealed a cyber ransom attack on a high-tech company, highlighting the "threats to national security" and the "importance of vigilance" against overseas cyber extortion. https://www.globaltimes.cn/page/202403/1309258.shtml

Network attacks

Attacks by China

- 2006. Chinese hackers were thought to be responsible for shutting down the House of Commons computer system. https://www.information-age.com/china-hacks-uk-government-20255/

- May 2008. The Times of India reported that an Indian official accused China of hacking into government computers. The official stated that the core of the Chinese assault is the scanning and mapping of India's official networks to gain access to content in order to plan how to disable or disrupt networks during a conflict. https://www.financialexpress.com/archive/a-virtual-war-on-terror/305242/

- March 2010. NATO and the EU warned that the number of cyberattacks against their networks had increased significantly

over the past 12 months, with Russia and China among the most active adversaries. https://www.theguardian.com/world/2010/may/17/nato-faces-cyber-attacks-study.

- March 2013. Beginning in 2012, Chinese hackers targeted civilian and military maritime operations within the South China Sea, in addition to U.S. companies involved in maritime satellite systems, aerospace companies and defense contractors

- May 2013. Chinese hackers compromise the U.S. Department of Labor and at least nine other agencies, including the Agency for International Development and the Army Corps of Engineers' National Inventory of Dams. https://www.pcworld.com/article/451627/us-department-of-labor-website-infected-with-malware.html

- April 2017. Chinese attempts to penetrate South Korean military, government and defense industry networks continued at an increasing rate since a February announcement that the THAAD missile defense system would be deployed in South Korea https://edition.cnn.com/2017/04/27/asia/china-south-korea-thaad-hack/index.html

- July 2021. The United States, the European Union, NATO and other world powers released joint statements condemning the Chinese government for a series of malicious cyber activities. They attributed responsibility to China for the Microsoft Exchange hack from early 2021 and the compromise of more than 100,000 servers worldwide. https://www.reuters.com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19.

- December 2021. Hackers targeted multiple Southeast Asian governments over the past 9 months using custom malware linked to Chinese state-sponsored groups. Many of the nations targeted are currently engaged in disputes with China over territorial claims in the South China Sea. https://apnews.com/article/technology-business-indonesia-beijing-asia-bca3e5785c03cb4d7a1e3052f545a922

- A full list of such attacks have been compiled by the Center for Strategic and International Studies at this link https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000

Attack Against China

- September 2019. Huawei accused the U.S. government of hacking into its intranet and internal information systems to disrupt its business operations. https://www.bankinfosecurity.com/huawei-accuses-us-government-hack-attacks-a-13011

- July 2020. Media reports say a 2018 Presidential finding authorized the CIA to conduct cyber operations against Iran, North Korea, Russia, and China. The operations included disruption and public leaking of information https://www.yahoo.com/news/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html

Attacks on Critical Infrastructure

Attacks by China

- November 2011. According to a major U.S. news source, Chinese hackers interfered with two satellites belonging to NASA and USGS. https://eijournal.com/news/industry-insights-trends/nasa-earth-observation-satellites-hacked-by-china

- March 2012. NASA's Inspector General reported that 13 APT attacks successfully compromised NASA computers in 2011. In one attack, intruders stole 150 user credentials that could be used to gain unauthorized access to NASA systems. Another attack at the Joint Propulsion Laboratory involving China-based IP let the intruders gain full access to key JPL systems and sensitive user accounts. https://www.securityweek.com/nasa-inspector-general-said-hackers-had-full-functional-control-over-nasa-networks

- March 2021. Suspected Chinese hackers targeted electricity grid operators in India in an apparent attempt to lay the groundwork

for possible future attacks. https://www.hindustantimes.com/india-news/chinese-hackers-targeted-7-indian-power-hubs-govt-says-ops-failed-101649356540330.html

Supply Chain attacks

Attack by China

- October 2008. Police discovered a highly sophisticated supply chain attack where credit card readers made in China and used in UK supermarkets had a wireless device inserted in them. The device copies a credit card when it is inserted, stores the data, and transfers the data it has collected once a day via WiFi connection to Lahore, Pakistan. Estimated loss is $50 million or more. The device could be instructed to collect only certain kinds of cards (such as gold cards), or to go dormant to evade detection https://www.wsj.com/articles/SB122366999999723871

- December 2017. The state-owned China Aerospace Science and Industry Corporation (CASIC) is alleged to have pre-installed backdoors in biometric equipment sold to Taiwan for its e-Gate border control system. The backdoors would have allowed CASIC to gather private data on both Taiwanese and foreign citizens traveling in and out of the country since the system's installation in 2012. https://www.taipeitimes.com/News/front/archives/2017/12/04/2003683391

List of cyber incidents-United Kingdom

After the US NSA, the UK's GCHQ is believed to have the most advanced data surveillance and collection capabilities. The UK has also tried to sell itself as a data secure country where companies can be assured of having a secure cyberspace. However, that has not prevented large scale attacks on its networks and systems, especially from Russia based hackers. The UK has also acknowledged that it engages in offensive cyber operations but under strict operating protocols.

Network Attacks

- August 2007. The British Security Service, the French Prime Minister's Office and the Office of German Chancellor Angela Merkel all complained to China about intrusion on their government networks. Merkel even raised the matter with China's President. https://www.dw.com/en/china-rejects-renewed-accusations-of-cyber-spying/a-2836152

- September 2007. British authorities reported that hackers, believed to have come from China's People's Liberation Army, penetrated the network of the Foreign Office and other key departments. https://timesofindia.indiatimes.com/world/uk/chinese-hackers-raid-uk-govt-computers/articleshow/2341455.cms

- December 2010. British Foreign Minister William Hague reported attacks by a foreign power on the Foreign Ministry, a defense contractor and other "British interests" that evaded defenses by pretending to come from the White House. https://www.theguardian.com/technology/2011/feb/06/hacking-william-hague-munichhttps://www.theguardian.com/technology/2011/feb/06/hacking-william-hague-munich

- May 2012. UK officials told the press that there had been a small number of successful perpetrations of classified MOD networks. https://www.telegraph.co.uk/news/9244209/Hackers-should-be-rewarded-for-showing-defence-breaches-says-military-chief.html

- July 2017. GCHQ issued a warning saying that state-sponsored hackers had likely broken into the Industrial Control Systems of UK energy companies https://www.theguardian.com/technology/2017/jul/18/energy-sector-compromised-state-hackers-leaked-gchq-memo-uk-national-cybersecurity-centre

- March 2018. Cybersecurity researchers reveal that a Chinese hacking group used malware to attack the service provider for the UK government in an attempt to gain access to contractors at various UK government departments and military organizations

- April 2018. The director of the UK's Government Communications Headquarters (GCHQ) announced that the organization had been conducting offensive cyber operations against ISIS to suppress their propaganda, disrupt their coordination, and protect deployed military personnel https://www.bbc.com/news/technology-43738953

- June 2021. A spreadsheet was leaked containing classified personal details of the 1,182 United Kingdom's Special Forces soldiers on WhatsApp. https://www.theregister.com/2021/06/02/uk_special_forces_data_breach_whatsapp/

- June 2021. The U.S. and British governments announced the Russian GRU attempted a series of brute force access against hundreds of government and private sector targets worldwide from 2019 to 2021, targeting organizations using Microsoft Office 365® cloud services. https://www.thestatesman.com/world/nsa-discloses-russias-brute-force-hacking-methods-1502977991.html

- February 2022. The networks of the U.K. Foreign Office were penetrated by hackers. All details of the incident remain confidential. https://www.bbc.com/news/technology-60309335

- August 2023. A cyber-attack on the UK Electoral Commission exposed voter data from 2014-2022. The breach included names and addresses. The UK imposed sanctions against Chinese actors

in May 2024. https://www.bbc.com/news/uk-politics-68654533

- May 2024. A cyberattack on Britain's military exposed personal details of thousands of soldiers. Officials said they suspect Chinese hackers, but China denied involvement, calling the accusations "absurd" and "malicious slander. https://www.voanews.com/a/china-suspected-of-cyberattack-on-britain-s-military/7601972.html

Notable cyber incidents-Israel

Israel has been facing the brunt of cyber attacks from hostile actors that parallel what has been taken place offline. There have been considerable attacks on critical infrastructure with the frequency and intensity of these attacks escalating over the years. 4th part in Israel has also engaged in offensive and pre-emptive cyber attacks on both state and non state actors.

Cyber-espionage

- September 2007. Israel disrupted Syrian air defense networks (with some collateral damage to its own domestic networks) during the bombing of an alleged Syrian nuclear facility. https://www.reuters.com/article/world/israel-admits-bombing-suspected-syrian-nuclear-reactor-in-2007-warns-iran-idUSKBN1GX09P

- January 2009. Hackers attacked Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip. The attack, which focused on government websites, was executed by at least 5,000,000 computers. Israeli officials believed the attack was carried out by a criminal organization from the former Soviet Union and paid for by Hamas or Hezbollah. https://www.theguardian.com/technology/2009/jan/15/israel-palestine-online-conflict

- October 2010. Stuxnet, a complex piece of malware designed to interfere with Siemens Industrial Control Systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear program. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

- May 2012. An espionage toolkit named "Flame" is discovered in computers in the Iranian Oil Ministry, as well as in other Middle Eastern countries, including Israel, Syria, and Sudan, and other nations around the world. https://www.zdnet.com/article/flame-most-complex-cyber-attack-ever-discovered/

- July 2012. A Trojan nicknamed "Mahdi" found gathering data from approximately 800 critical infrastructure engineering firms, government agencies, financial houses, and academia throughout the Middle East and beyond, predominantly in Israel and Iran. The virus contains Persian language strings. https://www.securityweek.com/mahdi-espionage-malware-targeting-systems-middle-east/

- January 2016. Israel revealed an operation by the United States and Britain to hack into Israel's surveillance drones. https://theintercept.com/2016/01/28/israeli-drone-feeds-hacked-by-british-and-american-intelligence/

- April 2017. The Israeli Cyber Defense Authority announced it had defended an Iranian cyberattack campaign against 120 targets in the government, high-tech, medical, and education sectors https://securityaffairs.com/58464/hacking/oilrig-apt-target-israel.html

- October 2018. News reports reveal that the Israel Defense Force requested that cybersecurity companies develop proposals for monitoring the personal correspondence of social media users. https://www.haaretz.com/israel-news/2018-10-16/ty-article/.premium/idf-worked-to-create-a-system-to-track-social-media-users-private-correspondence/0000017f-e89b-df5f-a17f-fbdf54ae0000

- March 2019. North Korean hackers targeted an Israeli security firm as part of an industrial espionage campaign. https://www.haaretz.com/israel-news/business/2019-03-26/ty-article/.premium/north-korean-hackers-cited-in-rare-attack-in-israel/0000017f-f833-d044-adff-fbfb9b020000

- March 2019. Iran's intelligence service hacked into former IDF Chief and Israeli opposition leader Benny Gantz' cellphone ahead of Israel's April elections. https://www.jpost.com/breaking-news/iranian-intelligence-hacks-benny-gantzs-phone-583453

- March 2019. Chinese hackers targeted Israeli defense firms that had connections to the U.S. military https://

www.middleeasteye.net/news/chinese-hackers-targeted-israel-large-scale-cyberattack-claims-firm

- May 2019. The Israeli Defense Forces launched an airstrike on Hamas after they unsuccessfully attempted to hack Israeli targets. https://www.cnbc.com/2019/05/06/israel-conflict-live-response-to-a-cyberattack-will-lead-to-a-shift.html

- October 2019. An Israeli cybersecurity firm was found to have sold spyware used to target senior government and military officials in at least 20 countries by exploiting a vulnerability in WhatsApp. https://www.bbc.com/news/technology-57881364

- August 2020. The Israeli defense ministry announced that it had successfully defended against a cyberattack on Israeli defense manufacturers launched by a suspected North Korean hacking group https://www.deccanherald.com/world/north-korean-hacking-group-attacks-israeli-defence-industry-872707.html

- August 2020. Hackers for hire suspected of operating on behalf of the Iranian government were found to have been working to gain access to sensitive information held by North American and Israeli entities across a range of sectors, including technology, government, defense, and healthcare.

- February 2021. Suspected Iranian hackers targeted government agencies in the UAE as part of a cyber espionage campaign related to the normalizations of relations with Israel. https://cyberscoop.com/suspected-iranian-hackers-snooping-on-middle-eastern-targets-anew/

- August 2021. Hacks initially attributed to Iran in 2019 and 2020 were found to be conducted by Chinese operatives. The cyberattack broke into computers across Israel's government and tech companies. https://www.technologyreview.com/2021/08/10/1031622/chinese-hackers-false-flag-iran-israel-fireeye/

- October 2021. A group with ties to Iran attempted to hack over 250 Office 365 accounts. All the targeted accounts were either U.S. and Israeli defense technology companies, had a focus on Persian Gulf ports of entry, or maritime transportation

companies with a presence in the Middle East. https://therecord.media/microsoft-iran-linked-hackers-breached-office-365-customer-accounts

- March 2022, Israel's government websites were hit by a cyberattack, believed to be one of the largest ever, which was attributed to a denial of service (DDoS) attack https://www.aljazeera.com/news/2022/3/15/israel-says-government-sites-targeted-by-cyberattack-2

This monograph explores the varying approaches of the United States, China, Russia, the United Kingdom, and Israel towards military engagements in cyberspace, detailing their initial strategies, underlying expectations, and the resultant outcomes. By examining these diverse national strategies, the study provides insightful analysis into the evolving perspectives and practices regarding military involvement in cyberspace across different states.

Dr Cherian Samuel is a Research Fellow in the North America and Strategic Technologies Centre.

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