Threats from the Virtual Plane: Is India Prepared?

Jiten Jain[1] and Joy Mitra[2]

In May 2017, the global cyberspace encompassing many countries, including India were hit by a ransom malware WannaCry, which targeted computers using Microsoft Windows Operating System across nations, sectors and industries.[3] The malware targeted some 200,000 systems in a very short span of time,[4] by dint of its ability to not just affect individual systems

1 Jiten Jain is a leading cyber security expert specializing in geopolitical intelligence analysis and its mapping to global cyber security/conflict issues. He heads Indian Infosec Consortium, an independent not-for-profit organization and is a recipient of Chevening Fellowship by the British Government. He is the co-founder of Voyager Infosec and a visiting faculty at the National Police Academy and Foreign Service Institute of the Ministry of External Affairs.

2 Joy Mitra is a researcher with the South Asia Terrorism Portal. He writes on foreign policy, coercive bargaining, deterrence stability and security in South Asia. He is a recipient of the 2015-16 Foreign Policy Fellowship of the Youth Forum for Foreign Policy and the Jindal School of International Affairs, OP Jindal Global University.

3 Timothy B. Lee, "The WannaCry ransomware attack was temporarily halted. But it's not over yet", Vox, May 15, 2015, https://www.vox.com/new-money/2017/5/15/15641196/wannacry-ransomware-windows-xp

4 Matthew Broersma, "NSA Malware 'Infects Nearly 200,000 Systems'", Silicon, April 25, 2017, http://www.silicon.co.uk/security/nsa-malware-security-210253?inf_by=5a8aa493681db807128b51ee

but also to infect the entire networks.[5] The malware would, in effect, encrypt data on the victim's computer (Figure1) denying file access to the user on his/her own computer unless ransom was paid in Bitcoin crypto-currency. The attack was allegedly conducted by a hacking outfit, the Lazarus Group, believed to be under the state control of the Democratic People's Republic of Korea (North Korea).[6] Later public attribution was made by United States, United Kingdom, Australia, Canada, New Zealand and Japan, referring to the malware attack as a state sponsored cyber-attack by North Korea.[7]

The WannaCry attack holds important ramifications on how states perceive the cyber-threat spectrum. The foremost consideration is that cyber-attacks, like sub-conventional warfare, don't necessitate a declaration of war and can therefore be conducted not just during wartime but also peacetime. Second, if such cyber-paralysis is inflicted on the command and control unit of any Security Force or the operations room of a critical Government installation like air-traffic control during a real-time operation, the magnitude of risks it would pose to lives and national security is impossible to contemplate.

5 Zammis Clark, "The worm that spreads WanaCrypt0r", Malware Bytes, May 13, 2017, https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/

6 Dustin Volz., "U.S. blames North Korea for 'WannaCry' cyber attack", Reuters, December 19, 2017, https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q

7 "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea", Infrastructure & Technology, Press Briefings, The White House, United States, December 19, 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

Figure 1: Screenshot of the WanaCry Decryptor Tool[8]

Significantly, in 2009, a malware called Conficker infected both the civil and defence establishment in the United Kingdom (UK), including computer systems of ships, submarines and establishments of the Royal Navy as well as well as a number of Royal Air Force Stations.[9] The same malware also forced French air operations to be suspended.[10]

Third, if outfits under the aegis of the state have the capability to execute such attacks, the potential for damage and irrational aggressive behaviour increases because of the higher qualitative and quantitative resources that an aggressor state can muster. Fourthly, states can provide immunity against legal or other means of retribution by claiming sovereignty.

The probability that damage from such attacks is not limited to the virtual plane alone, and may also result in

8 Anonymous, "WannaCry ransomware used in widespread attacks all over the world", Securelist, May 12, 2017, https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/

9 Lewis Page, "MoD networks still malware plagued after two weeks", The Register, January 20, 2009, https://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong/

10 Kim Willsher, "French fighter planes grounded by computer virus", The Telegraph, February 7, 2009, https://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html

potential physical damage, is dangerously high and increasing, with entire ecosystems of governance, business, services and personal lives becoming more cyber enabled and technology dependent. This diffusion of technology followed by dependency on information highlights the vulnerability that exists if such systems are compromised, either individually or in unison. This vulnerability creates incentive for actors ranging from non-state actors comprising individuals and groups to state actors as well as outfits acting on behalf of the state, to exploit the cyber-space comprising information technology (IT) networks, computer resources, and all the fixed and mobile devices connected to the global Internet.[11]

In effect, this gives rise to a cyber threat spectrum. This cyber-threat spectrum does not exist in isolation, and its evolution has simultaneously been accompanied by merging the capability to launch such attacks with other forms of warfare. Effectively transforming the conflict spectrum not incrementally but in entirety, altering its very nature because what was earlier a discrete conflict spectrum has now become a conflict continuum.

Cyber-Nuclear-Conventional-Sub-conventional Continuum

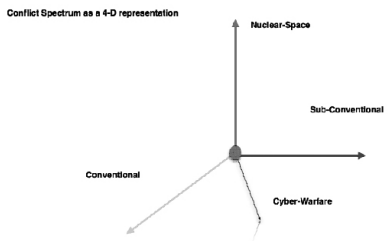

Figure 2. Four Dimensional Conflict Spectrum

11 Vittal Reddy, "Cyber security and challenges" The Hans India, June 14, 2017, http://www.thehansindia.com/posts/index/Young-Hans/2017-06-14/Cyber-security-and-challenges/306445

In the 1990s, prior to overt nuclearization, India's investments in conventional capabilities and its qualitative and quantitative edge appeared adequate to dissuade any extraordinary adventure on Pakistan's part. While the conventional deterrent operated with some success, Pakistan's asymmetric provocations as an offensive strategy made India fumble for answers, until it realised that its conventional deterrent could not account for the sub-conventional warfare that did not breach the conventional threshold. Before this point, India viewed a clear and discrete distinction between the nuclear-space, as well as conventional and sub-conventional zones of the conflict spectrum. In objective reality, however, the conflict spectrum had transformed into a continuum in the nuclear-conventional zone, effectively blunting India's conventional advantage.

India runs a similar risk, albeit of much higher proportions today, by failing to recognize the introduction of cyber-warfare in the conflict spectrum by its adversaries, and continuing to prepare only for patterns of warfare that have largely outlived their utility. Civic infrastructure, communications, defence, governance – there is hardly a segment that is untouched by IT or the cyber revolution. Along with business and related everyday activities, the dependency on technology has increased exponentially in warfare and in operations short of war, as well.

Any upgradation in technology accompanies almost an immediate change in the means of warfare because much of decision-making in warfare inevitably and invariably depends on information that is gleaned, processed, distributed, transmitted and looped faster than by the adversary. Cyber developments can interject in this cycle at any of these stages to either improve or impede decision-making ability. Importantly, cyber operations don't necessarily need to be limited in scope or intent in the cyber-space and can be powerfully combined with other means of warfare. Simultaneous or parallel execution of

capabilities gives rise to a multi-dimensional spectrum, and discrete levels in the conflict are replaced by a continuum.

The conflict spectrum (Figure 2) has essentially transformed into a 4-dimentional space with cyber (í) being the fourth dimension in what was earlier a 3-dimentional nuclear-space (ń), conventional (ć) and sub-conventional (ś) axes spectrum. Any point in the conflict-spectrum will therefore be defined by not just the traditional three attributes, but four. The continuum can refer to simultaneous or parallel warfare in more than one dimension of the 4D conflict spectrum, in effect merging two or more forms of warfare. With the advent of cyber warfare it is possible for a conflict point to exist simultaneously in cyber and the sub-conventional; cyber and conventional; cyber and nuclear-space planes or in spaces comprising cyber, sub-conventional and conventional; cyber, sub-conventional and nuclear-space; and finally, the cyber, sub-convectional, conventional and nuclear-space.

Cyber Sub-Conventional Interface: More Probable, More Powerful

The Cyber-Sub-Conventional Interface refers to the use of cyber-warfare in conjunction with different forms of warfare below the conventional threshold, that are limited politico-military struggles to achieve political, social, economic or psychological objectives. Within the conflict lexicon, there are many terms that define different conflicts by combining elements of asymmetry, irregular tactics, deception, plausible deniability and use of advanced military platforms. Table 1 gives a summary of terms and different modes of warfare, their intersection with cyber and information technology along with conflicts in contemporary times that exemplify their nature.

Table 1. Summary of Terminology related to Sub Conventional Warfare

Term	Definition	Intersection with Cyber /Information Technology	Example
Sub-Conventional Warfare	A generic term used to A generic term used to describe all armed conflicts that are below the threshold of war and above the level of peaceful co-existence amongst states [12]. It is a broad spectrum of military and Para-military operations, normally of long duration, predominantly conducted by indigenous or surrogate forces organized, trained, equipped, supported and directed in varying degrees by an external source during all conditions of . war or peace[13]	Yes	All insurgencies and terrorism related conflicts and violence barring conventional wars between states.
Political Warfare	The term is contested; George Keanon defined it as employment of all means short of war, to achieve its national objectives, ranging from overt actions: political	Yes	Pakistani information warfare in Kashmir fanning violence the population[14]

12 K. C. Dixit, "Sub-Conventional Warfare Requirements, Impact and Way Ahead", Journal of Defence Studies, Volume 4, Number 1, 2009, p. 121, https://idsa.in/system/files/jds_4_1_kcdixit.pdf

13 Ibid, p. 121

14 Amit Khajuria, "Pakistan intensifies cyber warfare over Kashmir" The Tribune, April 22, 2017, http://www.tribuneindia.com/news/jammu-kashmir/community/pakistan-intensifies-cyber-warfare-over-kashmir/395539.html

	alliances, economic measures and "white" propaganda to cover covert operations like clandestine support of "friendly" foreign elements, "black" psychological warfare and encouragement of underground resistance in hostile states[15]. Hoffman however calls the term imprecise as anything without the conduct of physical violence and limited to political and economic activities is not warfare[16].		
Psychological Warfare	Psychological Operations support tactical and strategic informational and propaganda objectives and used to embarrass, discredit, demoralise, divide and confuse the adversary [17].	Yes	Russian interference in US 2016 elections by posing as political activists and spreading discord[18]

15 "George F. Kennan on organizing political warfare", April 30, 1948, History and Public Policy Program Digital Archive, Wilson Centre, https://digitalarchive.wilsoncenter.org/document/114320

16 Frank Hoffman, "On Not-So-New Warfare: Political Warfare vs. Hybrid Threats", War on the Rocks, July 28, 2014, https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/

17 "Russian Military Power - Building a Military to Support Great Power Aspirations", Defence Intelligence Agency, Government of United States of America, 2017, http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf

18 Matt Apuzzo and Sharon La Franiere, "13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign", The New York Times, February 16, 2018, https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html

Asymmetric Warfare	Asymmetry refers to substantial difference between the capabilities of the opposing actors involved in the conflict. This asymmetry apart from the difference in force strength, weapons, and military prowess, also implies a difference in tactics and strategies employed, between the weaker and the stronger side. Most Insurgencies employ asymmetric warfare for their objectives.	Yes	Hezbollah's cyber warfare against Israeli critical infrastructure[19]
Unconvention	Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area[21].	Yes	Pakistan's support to Afghan Taliban operations in Afghanistan[20]
Law-fare	Actors, usually states, use legal means to delegitimize the strategic or tactical	Yes	Chinese manipulation of legal

19 Quoted in Levy Maxey, "Hezbollah goes on the Cyber Offensive with Iran's help", The Cipher Brief, January 30, 2018, https://www.thecipherbrief.com/hezbollah-goes-cyber-offensive-irans-help

20 Praveen Swami, "How Directorate S, ISI's most diabolical branch, outsmarted US in Kabul, continued subverting India", The Print, February 24, 2018, https://theprint.in/book-worm/failure-of-us-curb-isi-afghanistan-valuable-lesson/37710/

21 "DOD Dictionary of Military and Associated Terms, February 2018", Department of Defence, Government of United States of America, 2018, p.239, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-02-21-153603-643

	stance of the adversary, which sometimes can extend to even aiding or providing legal cover for physical operations or bargaining from a position of strength in an internationalised conflict. However this is not a form of warfare on its own and generally aids warfare in other forms.		arguments to undermine the opponent's information-control capabilities[22]
Grey-Zone Warfare	Grey-zone warfare defines inter-state conflicts that are left of centre in the spectrum of total war and peaceful relations. They combine elements of asymmetry, insurgency, irregular warfare and direct use of advanced military assets but keep the role of the sponsoring state actors ambiguous. This ambiguity also exists in the level and intensity of violence.	Yes	Russian annexation of Crimea, by encouraging civil war and separatism in the population[23]
Shadow Warfare	Wars fought without State attribution, leveraging social media to a high	Yes	US support for Syrian Rebels against Asad

22 Anonymous, "Doklam Stand-Off: Global Times Continues To Warn India, Is Beijing Waging Psychological Warfare Through Its Media?", Outlook India, July 25, 2017, https://www.outlookindia.com/website/story/doklam-stand-off-chinese-state-media-warns-time-for-a-second-lesson-for-forgetfu/299782

23 David Barno and Nora Bensahel, "Fighting and Winning in the 'Gray Zone'", War on the Rocks, May 19, 2015, https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/

	degree.[24]		Regime[25]
Hybrid Warfare	Simultaneous employment of conventional weapons, irregular tactics, terrorism and criminal behaviour in the same time and battlespace to obtain political objectives.[27]	Yes	Russian conduct of war in Ukraine[26]
Unrestricted	A sort of warfare in which all non-war actions transcending all boundaries and limits can be deployed towards achieving aims in an environment where information is omnipresent and the battlefield is everywhere, blurring the distinction between war and non-war, military and non-military.[28]	Yes	Russian blockage of Georgia Government and Media Websites, and disrupting telephones and communication networks just before the conflict over South Ossetia[29]

24 David Barno, "The Shadow Wars of the 21st Century", War on the Rocks, July 23, 2014, https://warontherocks.com/2014/07/the-shadow-wars-of-the-21st-century/

25 Mark Mazzetti and Michael C. Schimdt, "Behind the Sudden Death of a $1 Billion Secret C.I.A. War in Syria", The New York Times, August 2, 2017, https://www.nytimes.com/2017/08/02/world/middleeast/cia-syria-rebel-arm-train-trump.html

26 Mark Landler and Michael R. Gordon, "NATO Chief Warns of Duplicity by Putin on Ukraine", War on the Rocks, July 8, 2014, https://www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html?_r=0

27 Frank Hoffman, op. cit.

28 Qiao Liang and Wang Xiangsui, Unrestricted Warfare, 1999, PLA Literature and Arts Publishing House, Beijing, pp. 1-9, Translated from Mandarin to English, http://www.cryptome.org/cuw.htm

29 Manu Kaushik and Pierro Mario Fitter, "Beware of the bugs", Business Today, February 17, 2013, https://www.businesstoday.in/magazine/features/india-cyber-security-at-risk/story/191786.html

The role cyber and information technology play in almost all manifestations of sub-conventional war is evident. They may be used to shape the psychology and perception of the conflict by conducting information operations[30] to divide, terrorise, subvert and influence populations and actors, or support or limit or confuse politico-military decision making ability of the command. Or they could be used in collecting technical intelligence and for electronic warfare not just by state-actors but by militant or insurgent outfits who either exude such capability in terms of capable individual(s) or competent organisations. These actors could then maximise the use of technical intelligence available to them to launch daring sub-conventional assaults or could launch stand-alone cyber-attacks that can cause disruptions that are detrimental in terms of high magnitude physical and life-threatening damage that they cause.

Distributed Denial of Service (DDoS) attacks against Government services, water, electricity or power infrastructure, gas or oil distribution or delivery networks, telecommunications, banking or financial services, can paralyse the state, laying the ground for political instability and, potentially, physical conflict. The cyber-conventional and cyber-sub-conventional interfaces are the more probable and impactful machinations in this context, because cyber-space has become a necessary part of the conflict spectrum. Engaging and preparing for parallel warfare in two or more interfaces of the conflict spectrum is, consequently, now an urgent imperative.

30 "Field Manual No. 3-13 Information Operations: Doctrine, Tactics, Techniques, and Procedures", Headquarters, US Army Training and Doctrine Command, Department of the Army, Government of United States of America, November 28, 2003, https://fas.org/irp/doddir/army/fm3-13-2003.pdf

Strava[31] Heat Map Attack

Strava is a fitness app that markets itself as a social networking site for athletes. This seemingly harmless application tracks and maps user's running, cycling, jogging and other workout activity using the Global Positioning System (GPS) enabled on their phones or any other device, including a tablet or phablet with the GPS feature, to generate a heat-map of activity by all users. Strava also generates stats related to individual activity, accessible to the individual user. The heat map essentially shows all users of Strava globally, with the location of all the rides, runs, swims, and downhills that its users have taken, as collected by their smartphones and wearables.[32] Strava's database, however, has information on individual users that is not publicly accessible through the heat map, but is accessible to the users or employees of Strava or that could be accessed by a hacker in case of a potential privacy/data breach.[33] This data allows one to gain insight into an individual user's pattern of daily movement.

The publicly available heat map is enough to allow intelligent users to locate secret military installations or bases as happened in the case of Nathan Ruser, who used the heat map to identify US military forward bases in Afghanistan, Turkish military patrols in Syria, etc., by cross-referencing such heat maps with available Open Source Intelligence (OSINT), and Google Maps. Most of the modern military and non-military installations of Western countries in developing

31 "Global Heatmap", Strava, https://labs.strava.com/heatmap/#7.00/-120.90000/38.36000/hot/all

32 Ibid

33 Jeffrey Lewis, "Fitness-Tracker App Exposes Security Flaw at Taiwan's Missile Command Center", The Daily Beast, January 28, 2018, https://www.thedailybeast.com/strava-fitness-tracker-app-exposes-taiwans-missile-command-center?source=twitter&via=desktop

countries can be located with the help of these resources[34]. This is partly possible because, in certain locations like Afghanistan, Syria or Djibouti, Strava users are exclusively foreign military personnel, with the result that such military sites stand out on the heat map. In one of these cases a US Forces base and its layout in the Helmand Province was clearly visible on the heat map[35], although it was not visible on the satellite imagery of commercial providers like Google or Apple maps[36].

Figure 3. Military Base in Helmand Province, Afghanistan with route taken by joggers highlighted by Strava[37].

The more dangerous revelations could, however, come from the Strava activity data which could be used to tag and track persons of interest when these locations are revealed.

34 Jeremy Hsu, "The Strava Heat Map and The End of Secrets", Wired, January 29, 2018, https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

35 Alex Hern, "Fitness tracking app Strava gives away location of secret US army bases", The Guardian, January 28, 2018, https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

36 Ibid

37 Ibid

This is particularly relevant to missile bases or any other such installation where the security staff on duty change shifts. Security personnel if they use the app and their physical activity is tracked, can reveal locations of not just one but multiple bases, as and when these personnel are deployed on duty to different secret military installations in shifts.

Smesh

Smesh was a communication/chat application available free of cost on the Google Applications Store, offering end-to-end encryption and high quality voice calling over low data. At the time this application was popular among Defence Personnel in India and offered services that were fairly ahead of their time and not available in other applications that belonged to its category. When the code behind this application was reverse engineered[38] by one of the authors of the present paper (Jiten Jain) the data was found to be transmitted to a particular domain bought in the name of 'Sajid Rana' in Karachi, Pakistan. When a user installed the application on his phone, the app compromised the device, picked up all location related attributes, videos, photos and also recorded calls. But it went further in that it could also record sounds in the environment even whilst the phone was switched off, in effect turning the phone into an espionage device. Reverse engineering the source code of the Smesh app helped locate and identify actors within Pakistan who operated the application through a control panel, in essence removing the problem of attribution.

Physical Intelligence Gathering through Cyber-Space

On February 8, 2018, an Indian Air Force (IAF) Officer Group Captain Arun Marwaha was arrested by the Delhi Police

38 Reverse Code essentially implies breaking into the application code to view its internal logic and behavior and fully dissecting or deconstructing the underlying programming and application layers

Special Unit on charges of espionage and passing on classified information to Pakistani intelligence agency (Inter-Services Intelligence)[39]. The IAF officer in question was honey-trapped when he befriended ISI agents with fake profiles on social media, to the extent of exchanging intimate messages and pictures and subsequently passing sensitive defence information via social media. The information that he shared was reportedly on new agencies in the field of cyber warfare, space and special operations[40]. According to reports, Marwaha was engaging in espionage by taking unauthorised devices into restricted premises without permission[41]. This cyber honey trapping incident highlights the threats electronic devices pose simply by virtue of their presence in or near sensitive premises and how cyber-space is used to intrude into protected spaces without putting the lives of any operatives at risk. Physical intelligence gathering is conducted by compromised or willing individuals who are either part of the politico-security machinery, or by means that otherwise mask the role of the foreign agency behind the act.

Inferences

These examples, reflecting a very wide range of vulnerabilities, highlight the conundrum faced by Security Agencies in the realm of cyber-sub-conventional; cyber-conventional or cyber-nuclear-space warfare. In a 4D conflict spectrum, there is no dichotomy between civilian and military

39 Saurabh Trivedi, "IAF officer arrested on espionage charge", The Hindu, February 9, 2018, http://www.thehindu.com/news/national/iaf-officer-arrested-for-espionage/article22700475.ece

40 Mukesh Singh Sengar and Neeta Sharma, "Air Force Officer Arrested In Delhi, Was Seduced By ISI Spies On Chat", NDTV, February 9, 2018, https://www.ndtv.com/india-news/air-force-officer-arrested-in-delhi-for-allegedly-spying-for-pakistans-isi-1810501

41 Ibid

targets and therefore security has to encompass both civilians and security personnel. The Smesh App was used by military personnel as well as their family members in equal measure, and either of them, due to their proximity to important persons or sensitive locations, could lead to serious physical security risks, including endangering the security of important installations and the lives of security personnel. In this sense these Apps don't differentiate between civilian and military personnel. Cyber-securing military personnel is, consequently, not enough; security risks persist as long as even civilians are vulnerable.

The risks posed by 'harmless' apps built by genuine service providers for willing subscribers are also immense. As the heat maps case highlights, Strava was only providing a valuable service to willing subscribers, but the use of these services came at the cost making users vulnerable to geo-tracking. If Strava is unable to protect its database or some intelligent user is able to exploit the publicly available heat map along with other OSINT sources, to identify persons of interest, the security of important installations along with the personnel manning them, is at risk.

The ability to conduct espionage and physical reconnaissance through cyber-space without putting operatives at direct risk of being caught and, in turn, avoiding attribution is another aspect of the problem.

Further, the risk of catastrophic physical attacks that could stem because of lack of preparedness for cyber warfare is very high. If a foreign agency engages in such tracking, this can have serious repercussions even beyond the sub-conventional realm, intruding into the sphere of nuclear and conventional deterrence. The location of missile bases could allow the aggressor to put into operation nuclear counter-force strategies and contemplate first-strike options leading to a deterrence

break-down. The aggressor could take out the defendant's key missile bases, or communication transmission stations, and consequently his ability to retaliate to missile strikes whether nuclear or conventional. Such a pinpointed surprise attack could neutralize a significant portion of the defendant's armoury or render his warheads useless.

Finally, while plausible deniability can successfully operate in cases like the Strava heat maps, the problem of attribution could be solved in certain other instances, such as the case of the Smesh App.

Tinderbox!

The inferences drawn above are important in identifying not only future risks but the tinderbox that India currently sits on:

Aadhaar is a project initiated by the Government of India under the Aadhaar Act 2016, under the purview of the Ministry of Electronics and Information Technology, to uniquely identify all residents of India using biometrics. It is a project on a massive scale that stores critical identity related data digitally, raising privacy concerns and, more importantly, the fear of a pervasive security state. But the risks here are even greater, given that the existence of such a digital database almost in a magnetic way attracts interested actors who could use it to their advantage, given India's weak pedigree of protecting citizen privacy and its electronic ecosystems in the banking and finance sectors.

Minister of State (MoS) for Electronics and Information Technology Alphons Joseph Kannathanam admitted, on December 20, 2017, in the Lok Sabha (Lower House of India's Parliament) that, till November 30, 2017, Aadhaar had been linked to 252 schemes from various Ministries and Departments

and, until the day of his statement, 30 First Information Reports (FIR) had been filed by the Unique Identification Authority of India (UIDAI) with the Police for violation of the Aadhaar 2016 act.[42]

Further, on December 22, 2017, the Minister of State (MoS) for Electronics and Information Technology Alphons Joseph Kannathanam confirmed in the Rajya Sabha that two FIRs had been filed for allegedly attempting to breach the biometric authentication process of operators.[43]

On December 29, 2017 MoS Kannathanam confirmed further in the Rajya Sabha that 210 websites of the Central Government, State Government Departments and some educational institutions had published a list of beneficiaries along with their names, addresses and other details, with Aadhaar numbers, which were later removed.[44] Whether the Government took any penal action against its own departments for such casual handling of the data was not specified.

On January 8, 2018, Edward Snowden[45] tweeted in favour of a journalist who reported leakage of Aadhaar Data:

The journalists exposing the #Aadhaar breach deserve an award, not an investigation. If the government were truly

---

42 "Mandatory Aadhaar Linkage", Unstarred Question no. 819, Lok Sabha, Ministry of Electronics and Information Technology, Government of India, December 20, 2017, http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=58764&lsno=16

43 "Steps to protect UIDAIs iris scanbased security", Unstarred Question no. 896, Rajya Sabha Questions, Ministry of Electronics and Information Technology, Government of India, December 22, 2017, http://164.100.47.5/qsearch/QResult.aspx

44 "Publication of Aadhaar Details on government Websites", Unstarred Question no. 1364, Rajya Sabha Questions, Ministry of Electronics and Information Technology, Government of India, December 29, 2017, http://164.100.158.235/question/annex/244/Au1364.pdf

45 Tweeted by Edward Snowden, Twitter, January 8, 2018, https://twitter.com/snowden/status/950490382990790656?lang=en

concerned for justice, they would be reforming the policies that destroyed the privacy of a billion Indians. Want to arrest those responsible? They are called @UIDAI.

On January 21, 2018, Snowden tweeted again,[46]

Rarely do former intel chiefs and I agree, but the head of India's RAW writes #Aadhaar is being abused by banks, telcos and transport not to police entitlements, but as a proxy for identity – an improper gate to service. Such demands must be criminalized.

Risk perceptions, however, must not be limited to petty cyber-crimes, and must encompass increasing vulnerabilities on the strategic front. Crucially, Aadhaar related data is replicated or scattered across State Resident Hubs,[47] increasing its vulnerability. The potential for havoc that can be unleashed if access to any one of these databases is gained by any foreign intelligence agency cannot be captured in military, economic or other terms.

As a prelude to an armed conflict adversaries could target Aadhaar as part of an overall strategy to target all critical infrastructure and services effectively crippling state machinery and blocking services for citizens.[48] More importantly Aadhaar information of a 'person of interest', if accessed by a hostile actor, could be seriously damaging, as in the case Strava users revealing information about sensitive locations and interactions. If, for instance, the entry into these

46 Tweeted by Edward Snowden, Twitter, January 21, 2018, https://twitter.com/Snowden/status/955050455490547712

47 Nikhil Pahwa in "Aadhaar Will Turn India Into A Surveillance State, Say Petitioners", Left, Right and Centre, NDTV, January 17, 2018, https://www.ndtv.com/video/news/left-right-centre/aadhaar-will-turn-india-into-a-surveillance-state-say-petitioners-476844

48 Arun Mohan Sukumar, "The National Security Case Against Aadhaar", The Wire, March 2017, https://thewire.in/featured/national-security-case-aadhaar

sensitive locations is authenticated through Aadhaar it creates space for physical intrusion by hostile elements.[49] This could lead to physical intelligence gathering or even highly damaging kinetic attacks.

Stuxnet was a malware developed by the United States and Israel (though this has never been officially acknowledged) targeting Iranian nuclear centrifuges by issuing specific commands to the industrial control hardware responsible for their spin rate.[50] Stuxnet was supposedly meant to target only Iran's Natanz refining facility, which was air-gapped from outside networks and physical access to the network was therefore difficult. Getting the malware to the Natanz's network took all of a thumb drive, through spies and unsuspecting accomplices. The challenge was only to penetrate un-secure connected general networks.[51] It is significant that the Nuclear Power Corporation of India (NPCI) is forced to block at least ten targeted cyber-attacks a day.[52] Attackers only need to be successful once though, for a catastrophe to happen. It may not necessarily be the security of the target entity itself but any other unprotected private entity that may compromise the security of particular critical infrastructure.

Indian railway and airports traffic management centres could be potential targets for highly damaging physical attacks. Hacking into the railway traffic management system could

49 Ibid

50 Nate Anderson, "Confirmed: US and Israel created Stuxnet, lost control of it", Ars Techinca, January 6, 2012, https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

51 Sunil Abraham, Elonnai Hickok and Tarun Krishnakumar, "Security: Privacy, Transparency and Technology", CyFy Journal, Volume 2, 2015, pp. 107-115, https://cis-india.org/internet-governance/blog/security-privacy-transparency-technology.pdf

52 Ajai Sahni, "Trapped in past paradigms", India 2016, #689, January 2017, Seminar Web Edition, http://india-seminar.com/2017/689/689_ajai_sahni.htm

make it possible for a willing entity to crash trains into one another.[53] In 2011 a 'logic bomb' targeted the Common User Passenger Processing System (CUPPS) that performs many critical functions including managing reservation systems, check-in schedules and arrival and departure time of flights at Delhi Airport.[54] The attack completely disabled the system causing delays in flights and was essentially feasible because of insider access. Attacks of similar nature from an adversary state or non-state actor can lead to far more damaging consequences if they target metro, rail, road, port, air traffic or other transportation systems.

Slow Processing Putting National Security at Risk?

Moore's Law,[55] essentially an observation by Intel co-founder Gordon Moore in 1965, states that the number of transistors in a dense integrated circuit will continue to go exponentially. This necessarily implies that electronic devices rapidly condense into smaller size and exude higher levels of performance. Individual devices compute more powerfully and are able to do more. This has a direct bearing on the cyber-space where newer capabilities and technologies evolve in a disruptive way and are most often not anticipated by Governments, bureaucracies and other slow-response entities.

Unlike other domains where threats are generated on capabilities that are known or can be foreseen, in the new conflict spectrum, unforeseen and unprecedented threats loom

53 Manu Kaushik and Pierro Mario Fitter, "Beware of the bugs", Business Today, February 17, 2013, https://www.businesstoday.in/magazine/features/india-cyber-security-at-risk/story/191786.html

54 Vicky Nanjappa, "How techies used logic bomb to cripple Delhi airport", Rediff, November 21, 2011, http://www.rediff.com/news/report/how-techies-used-logic-bomb-to-cripple-delhi-airport/20111121.htm

55 Gordon E. Moore, "50 Years of Moore's Law", Intel, April 19, 1965, https://www.intel.in/content/www/in/en/silicon-innovations/moores-law-technology.html

large due to capabilities that exist in the dark, already exist, or are on the threshold of existence. The rate of evolution of technology is inevitably faster than the rate of response in the cyber-space for authorities. The nature of these threats, which are essentially and necessarily, unforeseen and unprecedented, present challenges for the political and bureaucratic systems and could be described in terms of an OODA (Observe Orient Decide Act) decision loop.

Cyber-warfare presents a challenge at the very 'observe' pillar of the decision loop of politico-bureaucratic entities, because it invariably operates in a space where capabilities, and actors carrying out those capabilities, sometimes including even the act itself, are hidden until they are discovered through the target/victim they strike. This presents a problem with the threat perception of the decision makers itself, where preparedness is lacking for threats that were essentially never part of the perceived conflict spectrum. According to a Mandiant Consulting report, the mean time an intruder remained in the victim's system undetected was 205 days in 2014 and 146 days in 2015,[56] indicating the extended period for which an intrusion can go undetected.

The orient, decide and act pillars of the decision loop, which commence after the nature of the threat has been deciphered, and the political, security or bureaucratic leadership implements the response/changes within the system, tend to have a low speed or rather inertia, of their own. In a 4D conflict spectrum, where the cyber plane uniquely plays an important role, the evolution of threat and capabilities pose a challenge in that, even if a threat is identified, the time to process the response by the political and bureaucratic systems, including the time to problematize, formulate, debate and decide an efficient response, assign

56 Sanatan Kulshrestha, "Cyber Warfare: A Perspective", Center for Land Warfare Studies, October 15, 2016, http://www.claws.in/1650/cyber-warfare-%EF%BF%BD-a-perspective-sanatan-kulshrestha.html

resources, develop regimes, institutions, etc., to counter such threats, is often too long. This is particularly and acutely the case in India. Worse, the pace at which the nature of the threat changes and reinvents itself in this type of environment implies that if the decision loops are slow, the responses are invariably and inevitably outdated by the time they come into being. The extended timeframe of this decision loop is itself a significant risk to national security. Moreover, speeding up the process may not be enough in a competitive game; the decision loop needs to be processed faster than the adversary's decision loop to defend against newer threats, maintaining a qualitative superiority that secures a denial 'qualitative certainty' in terms of cyber response capabilities.

Need for Deterrence in a 4D-Confict Spectrum

The anarchy prevalent in the international system and the jostling for power between the permanent five at the United Nations Security Council (UNSC) prevents the emergence of any international consensus on how to regulate cyber capabilities. The superpower rivalry in the conflicts in Syria, Ukraine and the South China Sea, has demonstrated very clearly that the world is far from a rule-based order on contemporary issues of conflict. These conflicts exemplify the importance of early intervention and of shaping the battlefield, both on the physical and virtual planes, to one's advantage. Global governance regimes like the UNSC have been found wanting in conflict-management, while resolution has been out of the question. Global cyber-space like the international system is largely about actors helping themselves in the absence of institutions and global governance regimes that have a mechanism for conflict management.[57]

57 Anthony Craig and Brandon Valeriano, "Realism and Cyber Conflict: Security in the Digital Age", in Davide Orsi, J.R. Avgustin and Max Nurnus ed., Realism in Practise: An Appraisal, February 3, 2018, E-International Relations, p. 88, http: // www.e-ir.info/2018/02/03/realism - and-cyber-conflict-security-in-the-digital-age/

In future conflict, cyber warfare will be an essential part of the spectrum. Cyber warfare could be a prelude or the crux of the script, depending on the objectives of the attack. State actors like the US and China have dedicated cyber-security commands that deploy offensive and defensive cyber-warfare capabilities. The cyber realm may also be a realm of no allies, as the case of US PRISM has shown that, if the servers of the service providers are beyond the purview of local laws then there is essentially a no holds barred confrontation in terms of the data that is exposed to security or Government agencies of the host Government.[58] Allies, enemies and frenemies are treated alike. Similarly, the Chinese have a dedicated military Unit 61398 in the People's Liberation Army (PLA) for cyber-espionage, informational and network warfare[59] and have targeted individual, private and public entities with impunity, in line with the objectives of State Owned Enterprises (SOEs).[60] India still does not have a dedicated Cyber-Security Command.

The combination of capabilities and anarchic order make for a compelling need to deter aggressive actions, especially when state sponsors of such actions exist.

Is Deterring Cyber-Aggression Possible?

In a 4D Conflict Spectrum there are two kinds of threat that emanate from Cyber Warfare. One is limited to the virtual plane, the other involves kinetic attacks. Deterrence must be examined at both these levels.

---

58 Glenn Greenwald and Ewen Mac A Skill, "NSA Prism program taps in to user data of Apple, Google and others" , The Guardian, June 7, 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

59 Gary Brown and Christopher D. Young, "Evaluating the US-China Cybersecurity Agreement, Part 2: China's Take on Cyberspace and Cybersecurity", The Diplomat, January 19, 2017, https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2-chinas-take-on-cyberspace-and-cybersecurity/

60 Ibid

Deterrence is not a straightforward concept in the virtual plane. Unlike pure nuclear or conventional deterrence, actors, attribution, communication and signalling in a four dimensional Conflict Spectrum are not always clear. More importantly the effects of a cyber-attack or the capabilities required to deter such attacks are not necessarily limited to the cyber plane, but could manifest in terms of economic, financial, diplomatic or military costs.

With the kind of electronic and cyber ecosystems that are in development and the ones already installed, India is vulnerable to attacks from an increasing number of cyber capable state and non-state actors.[61] The key infrastructure and entire ecosystems are dependent on information technology, and present India with a fait accompli to defend its physical and virtual assets against such attacks. Protecting its networks and ensuring data security for public and private entities, service assurance and reliability, needs investing in such capabilities.

However, investing in denial and defensive capabilities per se will not necessarily manifest as deterrence capability in the cyber domain. Unlike other forms of warfare, the cost of conducting aggressive cyber operations, especially those not including kinetic attacks, are significantly lower in equipment, legal, financial and human terms, than other forms of warfare where these can lead to exposure to risks, especially to personnel, and can be diplomatically costly. Investing in denial and defensive capabilities is necessary, but it will not per se deter actions on part of capable and resourceful state and non-state adversaries. So the concept of deterrence by denial in the cyber-domain cannot exist under the current circumstances, when incentives for attacking are very high.

61 "M-Trends: A View from the Frontlines", Mandiant, 2017, http://files.shareholder.com/downloads/AMDA-254Q5F/0x0x938351/665BA6A3-9573-486C-B96F-80FA35759E8C/FEYE_rpt-mtrends-2017_FINAL2.pdf

This is even more relevant in cases where attribution is not fixed and therefore, despite suspicion, neither the aggressor nor the defendant clearly communicates intent. It is difficult for any actor to communicate deterrence in such a scenario as the aggressor intends to cause damage using offensive capability, but also tries to mask his identity, effectively causing damage without necessarily achieving coercion. Investing in defensive denial and redundancy in the systems is, therefore, key to ensuring superiority against incoming cyber-attacks, and is more important than achieving a near-impossible or imperfect deterrence.[62]

Role of Law-fare in the Escalation Ladder

In the case where attribution is fixed, the deterrence equation changes radically because intent can now be communicated clearly from the aggressor as well as the defendant. The action taken by the aggressor in this case has a clear communication of causing damage or holding the defendant's assets at risk. The defendant can deter the aggressor's actions using offensive cyber capabilities, law-fare or diplomatic options. A prohibitive cost can be imposed on the aggressor with a clear communication of what actions are not acceptable and will certainly invite reprisal. Scope for deterrence by threat of punishment and imposing a balance of terror can be established in building up thresholds and limits to warfare in the virtual plane.

It is important that the 'punishment' or retaliation is graduated or calibrated to demonstrate the commitment of the defendant and escalatory potential of the aggressor's actions. In the cyber-domain this is a difficult task, because thresholds that

62 Martin C. Libicki, "Cyberdeterrence and Cyberwar", Rand Project Air Force, 2009, p.73, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

exist in the nuclear or conventional sphere are not automatically replicated in this domain. The cyber domain, like the sub-conventional, is largely without thresholds; however unlike the sub-conventional realm, attribution and intent are even more difficult to establish. This may or may not hold when parallel execution of capabilities in more than one dimension of the 4D conflict spectrum takes place. It is therefore an imperative that other means are established to build thresholds or pave the ground for subsequent measures of reprisal.

In 2018, after failing to impress upon the Chinese to desist from cyber-espionage through diplomatic channels, the US resorted to law-fare as a measure of escalation. The United States Department of Justice charged five People's Liberation Army (PLA) personnel for account hacking, economic espionage and other offenses directed at six American victims in the US nuclear power, metals and solar product industries.[63] The accused were identified as Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, all officers in PLA's Unit 61398.[64]

Interestingly despite being victim to numerous cyber-espionage attacks, not a single First Information Report (FIR) has been filed in any of the cyber-espionage cases in India. Although an FIR was filed in the Marwaha case, this was qualitatively different, because the espionage did not occur purely though cyber-space; rather it was a violation of India's

63 "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage", Office of Public Affairs, Department of Justice, Government of United States of America, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

64 Shannon Tiezzi, "US Indicts 5 PLA Officers For Hacking, Economic Espionage", The Diplomat, May 20, 2014, https://thediplomat.com/2014/05/us-indicts-5-pla-officers-for-hacking-economic-espionage/

Official Secrets Act (OSA), 1923, by an individual who had been compromised through the social media.

Perhaps the reason for not investing diplomatic capital or engaging in law-fare is the realisation that the anarchy that prevails in the intentional system and global cyberspace offers no effective option to secure justice or reparation. Not setting the process of investigation into motion, however, disallows India from bearing to affect any of the international treaties in cases, where significant detail and hard evidence can potentially be unearthed.

The importance of making this a mandatory practise cannot be overstated because the potential for cyber-espionage manifesting or leading to a follow-up physical attack has a high probability, given the increasing dependency of states and militaries on IT and cyber infrastructure. Here, law-fare introduces an additional step in the escalation-de-escalation ladder, providing for greater flexibility in deterrence choices for the defendant. This is especially true in cases where cyber warfare is not limited to espionage or the cyber domain; and where the intent is rather to cause dangerous physical damage. Wading into law-fare could credibly demonstrate that next step would be definite offensive action to cause unbearable damage to the adversary. The threat of mutual-hurt can build thresholds. It is necessary because pure defence is not an option in this Conflict Spectrum.

Retaliation in the 4D-Conflict Spectrum
Retaliation limited to the Cyber Domain
Law-Fare
Diplomacy

Figure 4. Escalation-De-escalation Ladder (Deterrence by Threat of Punishment)

Figure 4 above describes a basic escalation-de-escalation ladder that has the following four levels; Diplomacy, Law-fare, Retaliation limited to the virtual plane and Retaliation in the 4D Conflict Spectrum. Of these India needs to focus and develop capabilities on the second and third rungs of the ladder, to assure the adversary of a credible response. Law-fare inflicts reputational costs on the adversary, and can impose political and economic coercion. It is, moreover, a necessary step in persuading and signalling to the aggressor that future actions will provoke a definite retaliation[65]. Retaliation in the cyber domain would then demonstrate the will and capacity to cause physical damage, instilling fear of reciprocity in the aggressor. By and large, the deterrence should be designed to hold at the third rung of the ladder, because anything that escalates to the fourth rung will essentially be a failure of deterrence.

Conclusion

Parallel warfare in different segments of the conflict spectrum is no longer an imaginary scenario. Cyber-space has transformed the Conflict Spectrum from a discrete field to a continuum, where cyber-space's interaction with other forms of warfare is as real as it gets. The cyber-sub-conventional continuum is one of the more powerful iterations in this spectrum, and has greater probability and potential for powerful attacks.

Warfare can be limited in its objectives, geographical extent, duration, means (range of weapon systems) and intensity; but in a 4D conflict spectrum, where cyber-warfare is an essential complement or supplement to other forms of warfare, there

65 Martin C. Libicki, op. cit., p.110

are no limits of geography, duration, means or intensity. Unlike the physical spectrum, limits in the virtual world are difficult to establish, impose or uphold in the absence of order in the international system; and just like the physical world, thresholds in the virtual plane need to established, assessed and re-established over a period of time. This absence of limits extends to targetting civilian and military realm equally. Finally, investment in defensive capabilities is necessary, but is not sufficient; offensive capabilities are needed to assure hostile actors – both enemies and frenemies – that their physical assets are also held at gun-point. A balance of terror approach works best in the new Conflict Spectrum.