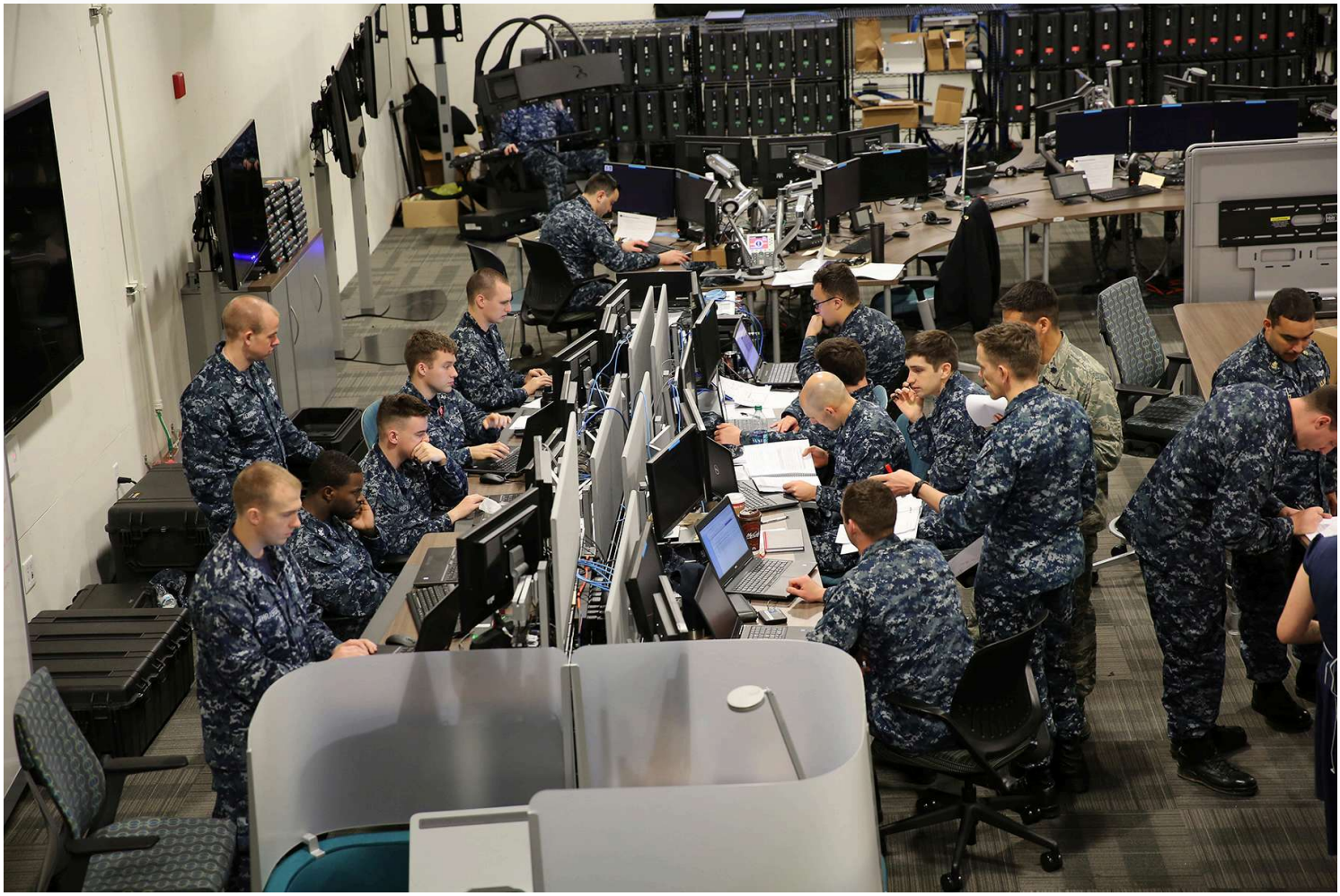
On cyber weapons and chimeras — by Gunjan Chawla and Vagisha Srivastava

CCG NLU, DELHI *on* SEPTEMBER 28, 2020

12 MINUTE READ



By Gunjan Chawla and Vagisha Srivastava

“The first thing we do, let’s kill all the lawyers,” says Shakespeare’s Dick the Butcher to Jack Cade, who leads fellow conspirators in the popular rebellion against Henry VI.

The same cliché may as well have been the opening line of Pukhraj Singh’s response to our last piece, which joins his earlier pieces heavily burdened with thinly veiled disdain for lawyers poking their noses into cyber operations. In his eagerness to establish code as law, he omits not only the universal professional courtesy of getting our names right, but also a basic background check on authors he so fervently critiques – only one of whom is in fact a lawyer and the other, an early career technologist.

In this final piece in our series on offensive cyber capabilities, we take exception to Singh’s misrepresentation of our work and hope to redirect the conversation back to the question raised by our first piece — what is the difference between ‘cyber weapons’ and offensive cyber capabilities, if any? Our readers may recall from our first piece in the series *Does India have offensive cyber capabilities* that Lt Gen. Pant had in an interview to Medianama, denied any intent on part of the Government of India to procure ‘cyber weapons’. However, certain amendments inserted in export control regulations by the DGFT suggested the presence of offensive cyber capabilities in India’s cyber ecosystem. Quoting Thomas Rid from *Cyber War Will Not Take Place,*

> *“these conceptual considerations are not introduced here as a scholarly gimmick. Indeed theory shouldn’t be left to scholars; theory needs to become personal knowledge, conceptual tools used to comprehend conflict, to prevail in it, or to prevent it.”*

While lawyers and strategists working in the cyber policy domain admittedly, still have a lot to learn from those with personal knowledge of the conduct of hostilities in cyberspace, deftly obscured by a labyrinth of regulations and rapidly changing rules of engagement, the question of nomenclature remains an important one. The

primary reason for this is that the taxonomy of cyber operations has significant implications for the obligations incumbent on States and State actors under international as well as domestic law.

A chimeral critique

Singh's most seriously mounted objection in his piece is to our assertion that 'cyber capabilities' and 'cyber operations' are not synonymous, just as 'arms' and 'armed attack', or 'weapons' and 'war' are distinct concepts. However, a wilful misunderstanding of our assertion that cyber capabilities and cyber operations are not interchangeable terms does not foster any deeper understanding of the legal or technical ingredients of a 'cyber operation' — irrespective of whether it is offensive, defensive or exploitative in intent and design.

The central idea remains, that a capability is wielded with the *intent* of causing a particular effect (which may or may not be identical to the actual effect resulting from the cyber operation). A recent report by the Belfer Center at Harvard on a 'National Cyber Power Index', which views a nation's cyber power as a function of its intent and capability, also seems to support this position. Certainly, the criteria and methodology of assessment remain open to debate and critique from academics as well as practitioners, and this debate needs to inform our legal position and strategic posture (again, the two are not synonymous) as to the legality of developing offensive cyber capabilities in international as well as domestic law.

Second, in finding at least one of us guilty of a 'failure of imagination', Singh steadfastly advocates the view that cyber (intelligence) operators like himself are better off unbounded by legal restraint of their technical prowess, functioning in a Hobbesian (virtual) reality where code is law and technological might makes right. It is thus unsurprising that Singh in what is by his own admission a 'never to be published manuscript', seems to favour practices normalized by the United States' military doctrine, regardless of their dubious legality.

Third, in criticizing lawyers' use of analogical reasoning — which to Singh, has become 'the bane of cyber policy' — he conveniently forgets that for those of us who were neither born in the darkness of covert cyber ops, nor moulded by it, analogies are a key tool to understand unfamiliar concepts by drawing upon learnings from more familiar concepts. Indeed, it has even been argued that analogy is the core of human cognition.

Navigating a Taxing Taxonomy

Writing in 2012 with Peter McBurney, Rid postulates that cyber weapons may span a wide spectrum, from generic but low-potential tools to specific high potential weaponry — and may be viewed as a subset of 'weapons'. In treating cyberweaponry as a subset of conventional weaponry, their underlying assumption is that the (cyber) weapon is being developed and/or deployed with 'the aim of threatening or causing physical, functional or mental harm to structures, systems or living beings'. This also supports our assertion that *intent* is a key element to planning and launching a cyber operation, but not for the purposes of classifying a cyber operation as an 'armed attack' under international law. However, it is important to mention that Rid considers 'cyber war' as an extremely problematic and dangerous concept, one that is far narrower than the concept of 'cyber weapons'.

Singh laments that without distinguishing between cyber techniques and effects, we fall into 'a quicksand of lexicon, taxonomies, hypotheses, assumptions and legalese'. He considers the OCOs/DCOs classification too 'simplistic' in comparison to the CNA/CND/CNE framework. Even if the technological underpinnings of cyber exploits (for intelligence gathering) and cyber attacks (for damage, disruption and denial) have not changed over the years, as Singh argues—the change in terminology/vocabulary cannot be attributed to 'ideology'. This change is a function of a complete reorganization and restructuring of the American national security establishment to permit greater agility and freedom of action in rules of hostile engagement by the military in cyberspace.

Unless the law treats cognitive or psychological effects of cyber operations, (eg. those depicted in the Social Dilemma or the Great Hack, or even in doxing classified documents) as harm that is 'comparable' to physical damage/destruction, 'cyber offence' will not graduate to the status of a 'cyber weapon'. For the time being, an erasure of the physical/psychological dichotomy appears extremely unlikely. If the Russian and Chinese playbook appears innovative in translating online activity to offline harm, it is because of an obvious conflation between a computer systems-centric cyber security model and the state-centric information security model that values guarding State secrets above all else, and benefits from denying one's adversary the luxury of secrecy in State affairs.

The changing legal framework and as a corollary, the plethora of terminologies employed around the conduct of cyber operations by the United States run parallel to the evolving relationship between its intelligence agencies and military institutions.

The US Cyber Command (CYBERCOM) was first created in 2008, but was incubated for a long time by the NSA under a peculiar arrangement established in 2009, whereby the head of the NSA was also the head of the US CYBERCOM, with a view to leverage the vastly superior surveillance capabilities of the NSA at the time. This came to be known as a 'dual-hat arrangement', a moniker descriptive of the double role played by the same individual simultaneously heading an intelligence agency as well as a military command. Simply put, cyber infrastructure raised for the purposes of foreign surveillance and espionage was but a stepping stone to building cyber warfare capabilities. Through a presidential memorandum in 2017, President Trump directed the Secretary of Defense to establish the US Cyber Command as a Unified Combatant Command, elevating its status from a sub-unit of the US Strategic Command (STRATCOM).

An important aspect of the 'restructuring' we refer to are two Presidential directives — one from 2012 and another from 2018. In October 2012, President Obama signed the Presidential Policy Directive — 20 2012 (PPD). It was classified as Top Secret at the time, but leaked by Ellen Nakashima of the Washington Post a month later. The PPD defined US cyber policy, including terms such as 'Offensive

Cyber Effects Operations' (OCEO) and 'Defensive Cyber Effects Operations' (DCEO) and mandated that all cyber operations were to be executed with the explicit authorization from the President. In August, 2018, Congress passed a military-authorization bill that delegated some cyber operations to be authorized by the Secretary of Defense. It is relevant that 'clandestine military activity (covert operations) or operations in cyberspace are now considered a traditional military activity under this statute, bringing it under the DoD's authority. The National Security Presidential Memorandum 13 (NSPM) on offensive cyber operations signed by President Trump around the same time, although not available in the public domain, has reportedly further eased procedural requirements for Presidential approval in certain cyber operations.

Thus, if we overcome apprehensions about the alleged 'quicksand of lexicon, taxonomies, hypotheses, assumptions and legalese,' we can appreciate the crucial role played by these many terms in the formulation of clear operational directives. They serve an important role in the conduct of cyber operations by (1) delineating the chain of command for the conduct of *military* cyber operations for the purposes of domestic law and (2) bringing the conversation on cyber operations outside the don't-ask-don't-tell realm of 'espionage', enabling lawyers and strategists to opine on their legality and legitimacy, or lack thereof, as military operations for the purposes of international law — much to Singh's apparent disappointment. To observers more closely acquainted with the US playbook on international law, the inverse is also true, where operational imperatives have necessitated a re-formulation of terms that may convey any sense of illegality or impropriety in military conduct (as opposed to the conduct of intelligence agencies, which is designed for 'plausible deniability' in case of an adverse outcome).

We relied on the latest (June 2020) version of JP 1-02 for the current definition of 'offensive cyber operations' in American warfighting doctrine. We can look to earlier versions of the DoD Dictionary to trace back the terms relevant to CNOs (including CAN, CNE and CND). This exercise makes it quite apparent that the contemporary terminologies and practices are all rooted in (covert) cyber intelligence operations, which the (American) law and policy around cyberspace

bends backwards to accommodate and conceal. That leading scholars have recently sought to frame 'cyber conflict as an intelligence contest' further supports this position.

- 2001 to 2007: 'cyber counterintelligence' as the only relevant military activity in cyberspace (even though a National Military Strategy for Cyberspace Operations existed in 2006)
    - 2008: US CYBERCOM created as a sub-unit of US STRATCOM
    - 2009: Dual Hat arrangement between NSA and CYBERCOM
    - 2010: US CYBERCOM achieves operational capability on May 21; CNA/CNE enter the DoD lexicon
    - 2012: PPD 20 issued by President Obama
    - 2013: JP 3-12 published as doctrinal guidance from the DoD to plan, execute and assess cyber operations
    - By 2016: DoD dictionary defines 'cyberspace operations', DCOs, OCOs, (but not cyberspace exploitation) relying on JP 3-12
    - 2018: NSPDM 13 signed by President Trump
    - 2020: 'cyberspace attack' 'cyberspace capability', 'cyberspace defence', 'cyberspace exploitation', 'cyberspace operations', cyberspace security, cybersecurity as well as OCOs/DCOs are defined terms in the Dictionary

Even as JP 3-12 remains an important document from the standpoint of military operations, reliance on this document is inapposite, even irrelevant for the purposes of agencies responsible for cyber intelligence operations. In fact, JP 3-12 is also not helpful to explain the whys and hows of the evolution in the DoD vocabulary. This is a handy guide to decode the seemingly cryptic numbering of DoD's Joint Publications.

Waging Cyber War without Cyber 'Weapons'?

It is relevant to mention that none of the documents referenced above, including JP 3-12, make any mention of the term 'cyber weapon'. A 2010 memorandum from the Chairman of the Joint Chiefs of Staff, however, clearly identifies CNAs as a form of 'offensive fire' – analogous to weapons that are 'fired' upon a commander's order, as well as a key component of Information Operations.

The United States' Department of Defense in its 2011 Defense Cyberspace Policy Report to Congress acknowledged that "the interconnected nature of cyberspace poses significant challenges for applying some of the legal frameworks developed for physical domains" and observed that "there is currently no international consensus regarding the definition of a cyber weapon".

A plausible explanation as to why the US Government refrains from using the term 'cyber weapons' is found in this report, as it highlights certain legal issues in the transporting cyber 'weapons' across the Internet through the infrastructure owned and/or located in neutral third countries without obtaining the equivalent of 'overflight rights', and suggests 'a principled application of existing norms to be developed along with partners and allies'. A resolution to this legal problem highlighted in the DoD's report to Congress is visible in the omission of the term 'cyber weapon' in legal and policy frameworks altogether, only to be replaced by 'cyber capabilities'.

We can find the rationale for and implications of this pivot in the work of Professor Michael Schmitt's 2019 paper, wherein he argues in the context of applicable international law – contrary to the position he espoused in the Tallinn Manual – that 'cyber capabilities' cannot meet the definition of a weapon or means of warfare, but that cyber operations may qualify as methods of warfare. This interpretation permits 'cyber weapons' in the garb of 'cyber capabilities' to circumvent at least three obligations under the Law of Armed Conflict/International Humanitarian Law.

First, is the requirement for legal review of weapons under Article 36 of the First Additional Protocol to the Geneva Conventions (an issue Col. Gary Brown has also written about) and second, is taking precautions in attack. Third and most

important, the argument that cyber weapons cannot be classified as munitions also has the consequence of depriving neutral States of their sovereign right to refuse permission of the transportation of weapons (or in this case, transmission of weaponised cyber capabilities) through their territory (assuming that this is technically possible).

So, in a sense, if we do not treat offensive cyber capabilities, or 'cyber weapons' as analogous in international law to conventional weapons normally associated with armed hostilities, in effect, we also restrain the ability of other sovereign States under international law to prevent and prohibit a weaponization of cyberspace without their consent, for military purposes of other cyber powers. Col. Gary Brown whose work Singh seems to nurture a deep admiration for admits that the first 'cyber operation' was conducted by the United States against the Soviet Union in 1982, causing a trans-Siberian pipe to explode by use of malware implanted in Canadian software acquired by Soviet agents. Since 1982, the US seems to have functioned in single-player mode until Russia's DDoS attacks on Estonia in 2007, or at the very least, until MOONLIGHT MAZE was uncovered in 1998. For those not inclined to read, Col. Brown makes a fascinating appearance alongside former CIA director Michael Hayden in Alex Gibney's 2016 Documentary 'Zero Days' which delves into Stuxnet — an obvious cyber weapon by any standards, which the US 'plausibly denied' until 2012.

Turning back to domestic law, the nomenclature is also significant from a public finance perspective. As anecdotal evidence, we can refer to this 2013 Reuters report, which suggests that the US Air Force designated certain cyber capabilities as 'weapons' with a view to secure funding from Congress.

From the standpoint of managing public perceptions too, it is apparent that the positive connotations associated with 'developing cyber capabilities' makes the same activity a lot more palatable, even development-oriented in the eyes of the general public, as opposed to the inherent negativity associated with say, the 'proliferation of cyber weapons'.

Additionally, the legal framework is also important to delineate the geographical scope of the legal authority (or its personal jurisdiction, if you will) vested in the military as opposed to intelligence agencies to conduct cyber operations. For organizational purposes, the role of intelligence would (in theory) be limited to CNE, whereas CNA and CND would be vested in the military. We know from (Pukhraj's) experience, this distinction is nearly impossible to make in practice, at least until after the fact. This overlap of what are arguably, artificially created categories of cyber operations, raises urgent questions about the scope and extent of authority the law can legitimately vest in our intelligence agencies, over and above the implicit authority of the armed forces to operate in the cyber domain.

Norm Making by Norm Breaking

In addition to understanding *who* wields offensive cyber capabilities, under what circumstances, it is also important for the law to specify *where* or *against whom* they are permitted to do so by law. Although militaries of modern day 'civilized' nations are rarely ever deployed domestically, there has been some recent concern over whether the US CYBERCOM could be deployed against American citizens in light of recent protests, just as special forces were. While the CIA has legal authority to operate exclusively beyond the United States, the NSA is not burdened by such constraints and is authorized to operate domestically. Thus, the governance/institutional choices before a State looking to 'acquire cyber weapons' or 'develop (offensive) cyber capabilities' range from bad to worse. One might either (1) permit its intelligence agencies to engage in activities that resemble warfighting more than they resemble intelligence gathering and risk unintentional escalations internationally or (2) permit its military to engage in intelligence collection domestically, potentially against its own citizens and risk ubiquitous militarization of and surveillance in its domestic cyberspace.

Even as many celebrate the recent Federal court verdict that the mass surveillance programmes of the NSA revealed by Edward Snowden were illegal and unconstitutional, let us not forget that this illegality is found vis-à-vis the use of this programme against American citizens *only* — not foreign surveillance

programmes and cyber operations conducted beyond American soil against foreign nationals. Turning to an international law analysis, it is the US' refusal to recognize State sovereignty as a binding rule of international law, that enables the operationalization of international surveillance and espionage networks and transmission of weaponized cyber capabilities that routinely violate not only the sovereignty of States, but also the privacy and dignity of targeted individuals (the United States does not accept the extra-territorial applicability of the ICCPR).

The *nom de guerre* of these transgressions in American doctrine is now 'persistent engagement' and 'defend forward', popularized by the Cyber Solarium Commission most recently — a cleverly crafted term that brings about no technical changes in the *modus operandi*, but disguises aggressive cyber intrusions across national borders as ostensible self-defence.

It is also relevant that this particular problem also finds a clear mention in the Chinese Foreign Minister's recent statement on the formulation of Digital Security rules by China. Yet, it is not a practice from which either the US or China plan to desist. Recent revelations about the Chinese firm Zhenhua Data Information Technology Co. by the Indian Express have only served to confirm the expansive, and expanding cyber intelligence network of the Chinese state.

These practices of extraterritorial surveillance, condemnable as they may be, have nonetheless, shaped the international legal order we find ourselves in today — a testimony to the paradoxical dynamism of international law — not unlike the process of 'creative destruction' of cyberspace highlighted by Singh — where a transgression of the norm (by either cyber power) may one day, itself become a norm. What this norm is, or should be still remains open to interpretation, so let's not rush to kill all the lawyers — not just yet anyway.

This article was first published on CCG-NLUD's blog. It has been cross-posted with the author's permission.

Read more:

- Does India have cyber capabilities? *by Gunjan Chawla*
- What are 'offensive cyber capabilities'? *by Gunjan Chawla and Vagisha Srivastava*
- 'National Cyber Security Strategy awaiting cabinet nod, will hopefully be released in October': Rajesh Pant
- 'Don't conduct mass surveillance against other countries,' China tells the world in its global initiative on data security

Support our journalism:

For You

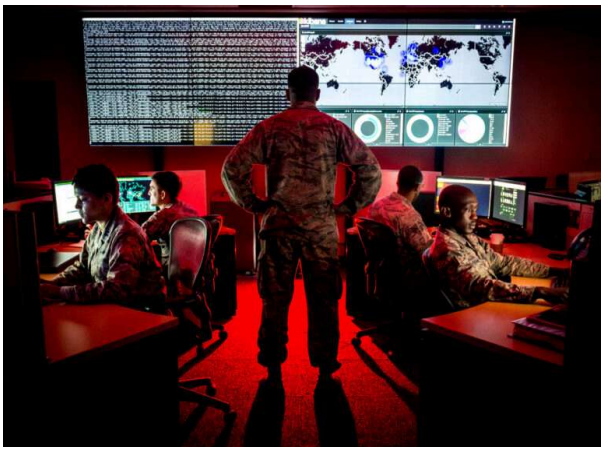
- **Sign up for our Daily Newsletter** to receive regular updates
- **Stay informed about MediaNama events**
- Have something to tell us? Leave an **Anonymous Tip**
- Ask us to **File an RTI**
- **Sponsor a MediaNama Event**

DISCOVER MORE

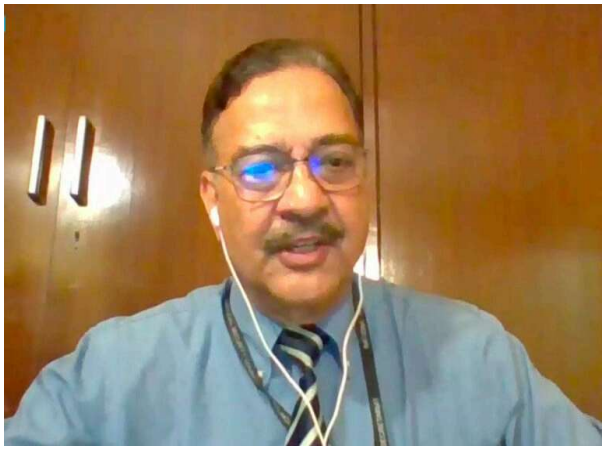
cyber security | cybersecurity | views

Related Posts:

Cybersecurity implications for the post COVID-19 era



What are 'offensive cyber capabilities'? — by Gunjan Chawla and Vagisha Srivastava



'National Cyber Security Strategy awaiting cabinet nod, will hopefully be released in October': Rajesh Pant

Exponential growth in number of cyber incidents reported to CERT-In during pandemic: MEITY

Summary: Tamil Nadu Cybersecurity Policy 2020

Does India have offensive cyber capabilities? — by Gunjan Chawla

MEDIANAMA

MediaNama is the premier source of information and analysis on Technology Policy in India. More about MediaNama, and contact information, here.