Vivekananda International Foundation

U.S. National Cyber Strategy and Department of Defence Cyber Strategy: An Analysis

Major General P K Mallick

VIF Brief
November - 2018

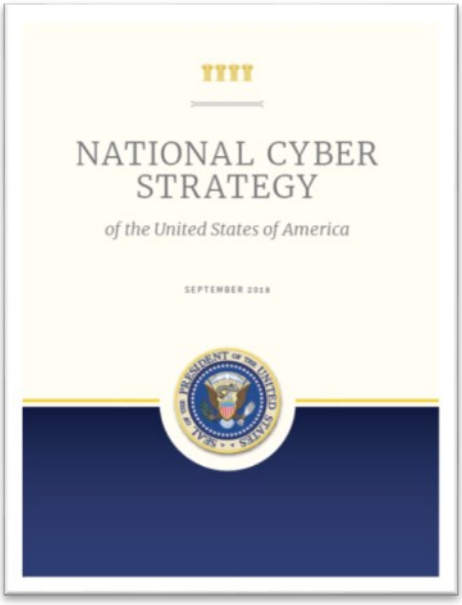
About the Author

Maj Gen PK Mallick, VSM (Retd) has been a Senior Directing Staff at the National Defence College, New Delhi. He is an expert in Cyber Warfare, SIGINT and Electronic Warfare and an observer of geo-political and economic trends. He is a member of the VIF Team as a Consultant.

U.S. National Cyber Strategy and Department of Defence (DoD) Cyber Strategy: An Analysis

Introduction

The Trump Administration released the 'National Cyber Strategy' on 20 September 2018. Around the same time, the 'Defense Department Cyber Strategy 2018' was also published. In the United States (U.S.), every government after taking over, announces some important policies and or strategy documents. The present administration has already released the 'National Security Strategy', the 'National Defense Strategy' and the 'Nuclear Posture Review'. The National Cyber Strategy was the last of the policy documents to be published as it went through a lot of deliberations before final and formal revelation.



Any nation's cyber strategy in today's interconnected world is of paramount interest as it affects government, commercial, scientific and educational infrastructures, including critical ones like for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services. The Department of Defence (DoD) has, therefore, a very important role to play in determining and formulating cyber strategy in any country. Since the United States of America is regarded as the sole super power and the biggest cyber power in the planet, its National Cyber Strategy and Defense Department Cyber Strategy would be read and analysed with keen interest.

The U.S. National Cyber Strategy

This strategy explains how the U.S. Administration will:-

- Defend the homeland by protecting networks, systems, functions and data.
- Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation.
- Preserve peace and security by strengthening the ability of the United States in concert with allies and partners- to deter, and if necessary, punish those who use cyber tools for malicious purposes.
- Expand American influence abroad to extend the key tenets of an open, interoperable, reliable and secure Internet.

For securing federal networks and information, the following priority actions have been identified:-

- Further centralise management and oversight of federal civilian cyber security.
- Align risk management and information technology activities.
- Improve federal supply chain risk management.
- Strengthen federal contractor cyber security.
- Ensure the government leads in best and innovative practices.

For securing critical infrastructure, the following priority actions have been identified:-

- Refine roles and responsibilities.
- Prioritise actions according to identified national risks.
- Leverage information and communications technology providers as cyber security enablers.
- Protect U.S. democracy.
- Incentivise cyber security investments.
- Prioritise national research and development investments.
- Improve transportation and maritime cyber security.
- Improve space cyber security.

President Trump claimed in his forwarding note that the United States now has its first fully articulated cyber strategy in 15 years. President George W. Bush issued the National Strategy to Secure Cyberspace in 2003. This is a little misleading. Though it wasn't styled as a 'strategy', President Barack Obama issued a detailed cyber space policy review within four months of taking office. He released the first international cyber space strategy in 2011 and issued multiple cyber focused executive orders and a cyber security action plan in 2016.

The reaction to the strategy document was largely positive across the political spectrum, from both Democrats and Republicans.

Some positive aspects of the National Cyber Strategy are as follows:-

- Re-states importance of Internet freedom and the central role of multi stakeholder internet governance, welcomes pronouncements to U.S. allies and partners.
- All tools of national power - diplomatic, law enforcement, economic, cyber and military - can be used to respond to a cyber incident. Offensive cyber operations are an important part of this arsenal.
- Emphasis on deterrence, including aspiring to impose 'swift, costly and transparent consequences when malicious adversaries harm the United States or its partners'.

- Collectively respond with a broader coalition of like minded states. To share threats by coordinating responses, intelligence, buttressing attribution, supporting each other's responses and engaging in 'joint imposition of costs against malign actors'.

Critics

It is expected that a strategy document like this would be detailed and ground breaking. Instead, it is general in nature, lacks detail and often restates past policies. In certain areas like articulating roles and responsibilities for federal agencies, it avoids mentioning hard issues, saying these will be worked out in the future.

Chris Painter, a former cyber coordinator for the United States State Department's cyber policy, said it is still not entirely clear how much leeway the Trump Administration will give offensive cyber operators and whether the strategy could succeed without a more public signal to targeted nation states like Russia, China, Iran and North Korea. He also expresses concern that in an all-out cyber war, the U.S. has more to lose than countries like China or Russia.

Congressman Jim Langevin, co-founder and co-chair of the Congressional Cyber Security Caucus and a senior member of the House Committees on Armed Services and Homeland Security, said, "But as the country with the most innovative economy in the world, we must also acknowledge the abiding interest of the United States in encouraging stability in this domain. It is incontrovertible that we must respond to malicious activity violating well established norms of responsible behavior, but that response must be whole-of-government and need not always include a cyber component." Langevin further said, "the document often fails to provide the strategic guidance regarding what trade-offs we should expect to make between regulating, supporting and responding to the needs of critical infrastructure owners and operators."

There are many unanswered questions. This strategy should not mean that offensive cyber operations will be the tools of first resort. Thee should be reserved for when they are most effective. The best response to a cyber attack is often not a cyber one. Cyber tools must be integrated into all capabilities and not seen as some sort of a magic button, particularly, given that their use involves a fair amount of pre-planning. Despite the borderless nature of cyber space, there is a difference if such tools are used in an adversary space, or if they are used to disrupt an adversary's activities in neutral or friendly territory.

In an adversary's space, the primary issue is escalation and that can be overcome with direct messaging. In a third party space, unilateral cyber actions run the risk of damaging alliances needed to take collective action against cyber and other threats, essentially making an international cyber deterrence initiative more difficult. There may be times when the U.S. may find the need to take unilateral action, but in other cases, it may be better to ask its allies to employ their capabilities. How these diplomatic and partnership issues will be weighted and resolved in the new structure needs to be explained. Failure to properly assess these issues risks loss of the ability to respond collectively to incidents in the long term.

The section on improving incident reporting and response states only that the government "will continue to encourage reporting of intrusions and theft of data by all victims." There should be a high level commitment to provide tangible incentives to entities that report cyber security incidents. National cyber strategy means additional authority to hack foreign countries. For the cyber security industry, the new American doctrine could mean a lucrative pay day. It allows for more offensive cyber operations and that Defense Department leaders "will make greater use of (commercial) capabilities that can be optimised for DoD use." The approach could lead to increased business opportunities for cyber security contractors.

Despite some positive signs, a few experts believe that the strategy falls short in the following key areas:-

- It does not adequately provide the Department of Homeland Security (DHS) with the needed directive authority and contains no direction that indicates that the DHS will be given the resources needed to 'own' the federal cyber security mission. The DHS remains a facilitator, collaborator, information sharer, etc.
- The document mentions cyber security of space as a focus area, but does not identify space as a national critical infrastructure or as an area requiring prioritised action.
- In the section on deterrence, it should have discussed cyber as an area that plays a key role in deterrence broadly instead of in the context of 'cyber deterrence'.
- The document should have placed primary importance on linking the need to ensure cyber resilience in overall critical infrastructure as a way to deny adversary benefit from cyber attacks. The document focusses on imposing costs on adversaries when they attack in the cyber domain. Cost imposition is important, but only when balanced against being resilient.
- Sufficient priority in key areas to indicate needed resources (funds and people) is not given.

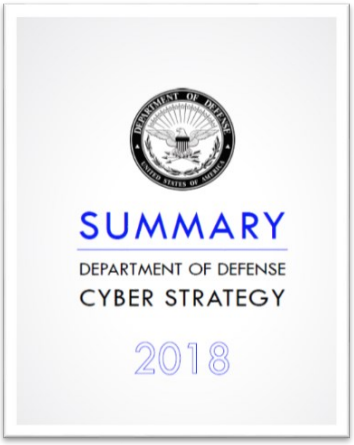
For U.S. administrations, seeking a way to strike back at adversaries, useful cyber weapons have been few and far between. Loosening legal restrictions may not be the answer. Under former President Barack Obama, National Security Council officials pressed government agencies for options to respond to widespread hacking and theft of intellectual property by foreign entities. The proposals that came back were often disappointing. Ari Schwartz, a former senior cyber security adviser in the Obama Administration, said, "In my experience, it has not been U.S. government deterrence policies that held back response, but the inability of agencies to execute,"

The apparent focus on use of offensive cyber tools has some lawmakers worried on grounds that it may invite painful retaliation. As one of the most wired global economies—reliant on the internet for Silicon Valley, energy generation, air traffic control, and more—the United States is a lot more vulnerable to cyber attacks than many of its potential adversaries. Inadvertent consequences, potential collateral damage, possible loss of control

and retaliation and escalation must all be considered. There is a need to develop and use these capabilities as part of an overall deterrence regime — but it is important that they be integrated and balanced as one of many strategic responses.

Too often, the cyber component is kept in a separate silo from other tools of national power. Cyber strategy specifies that all instruments of national power will be employed to deter malicious cyber activities. This implies the need for a more nuanced approach to countering the threat and understanding risks of escalation.

U.S. DoD Cyber Strategy



'Defense Department Cyber Strategy 2018', an unclassified summary and fact sheet were released on 18 September 2018. The full DoD document was not made available, but about six pages of content has been published in the form of an official 'summary'. The documents lay out a vision for addressing cyber threats and the priorities of the department's National Security Strategy and National Defense Strategy, which focus on a new era of strategic great power competition. The fact sheet shows what work the department has to do, particularly in the areas of workforce, capabilities and process.

After the announcement of the DoD cyber strategy in 2015 steps taken by the Defense Department are:-

- Has matured its cyber forces since 2015 by elevating the Cyber Command (CYBERCOM) to a Unified Command.
- Ensured maturation of 133 cyber national mission teams.
- Initiated the first public cyber campaign within a conventional conflict (Joint Task Force Areas, the cyber operations against ISIL in Syria).
- Delegated certain responsibilities of the President to the DoD to conduct cyber operations abroad.

The unclassified summary also calls out China and Russia as "long term strategic competitors" in cyber space, as well as North Korea and Iran, which "have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests." It wants to use the Pentagon's cyber capabilities to collect intelligence and prepare for future conflicts.

National Security Adviser John Bolton, just before the release of the DoD paper, said the following:-

- For any nation that's taking cyber activity against the United States, they should expect … responce offensively, as well as defensively. The United States cannot afford inaction.

- Create powerful deterrence structures that persuade the adversary not to strike in the first place.
- Decision making for launching some attacks will be moved down the chain of command; previously, offensive cyber operations generally required the approval of the President. Those envisioned in the new policy will include both offensive and defensive actions, only some of which may be made public.
- Actual offensive actions must still undergo rigorous examination to limit effects and to preclude perception of an act of war. Cyber conflict continues to be enormously complex.
- The goal is deterrence, to demonstrate to adversaries that the cost of their engaging in operations against us is higher than they want to bear. Adversaries need to know that the new policy to do a lot of things offensively is not because more offensive operations are wanted, but precisely to create structures of deterrence that will demonstrate to adversaries the cost of engaging in operations against U.S. will be higher than what they can bear.
- Effort is not to escalate cyber conflict, but to decrease it. The U.S. will identify, counter, disrupt, deter and degrade behavior in cyber space that is destabilising and contrary to its national interest.
- The current strategy is "very different from PPD-20" and America's "hands are not as tied as they were in the Obama Administration."

Key Themes of the Defence Strategy are:-

- Using cyber space to amplify military lethality and effectiveness.
- Defending forward, confronting threats before they reach U.S. networks.
- Proactively engaging in day-to-day great power competition in cyber space.
- Protecting military advantage and national prosperity.
- Recognising that partnerships are the key to shared success in protecting cyber space.
- Actively contesting exfiltration of sensitive DoD information.
- Embracing technology, automation and innovation to act at scale and speed.
- Supporting defence of critical infrastructure.
- Recruiting, developing and managing critical cyber talent.

The summary lists five objectives for the DoD's cyber space strategy. These are:-

- Ensuring the joint force can achieve its missions in a contested cyber space environment.
- Strengthening the joint force by conducting cyber space operations that enhance U.S. military advantages.

- Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident.
- Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks.
- Expanding DoD cyber cooperation with inter-agency, industry and international partners.

The strategy asserts that the U.S. Defense Department must be prepared to defend 'defense critical infrastructure', which it defines as "the composite of DoD and non-DoD assets essential to project, support and sustain military forces and operations worldwide as well as the defense industrial base. It will do this not by invoking defense support to civil authorities (a focus in the 2015 strategy), but instead by building trusted relationships with private sector entities that are critical enablers of military operations and carry out deliberate planning and collaborative training that enables mutually supporting cyber activities."

Implications of the 2018 Strategy are:-

- Places defence outside the bounds of the '.mil' (the networks owned and operated by the U.S. military) and instead advocates defence of resources that enable military operations but may operate on the .com (private industry).
- Expands departmental efforts beyond U.S. geographical boundaries. By instructing forces to halt activity at its source, the strategy advocates operations that degrade adversary cyber activity before those actions reach U.S. networks or assets.
- 'Defend forward' suggests a preemptive instead of a reactive response to cyber attacks. Reactive strategy might focus on hack-backs, while a preemptive strategy might focus on operations that prevent an adversary's cyber unit from accessing the Internet.
- The strategy asserts that the U.S. will be willing to take these actions before or after an armed conflict. This implies that restraint seen under the Obama Administration may no longer be the norm in Trump's Department of Defense.

Comparison between 2015 and 2018 Cyber Strategies

Former Defense Secretary Ash Carter had unveiled the Defense Department's cyber strategy on April 22, 2015. Factors which remain the same from the previous strategy are:-

- Both treat the open, free and reliable Internet as a foundational objective for U.S. national security.
- Both strategies accept that this open Internet may increase vulnerabilities, but also create prosperity and national security advantages that make those vulnerabilities a worthwhile risk. It represents a continued belief that the current structure of the Internet benefits the United States.
- Both strategies emphasise the role of increased cyber defence and resilience in ensuring the U.S. military's conventional war fighting superiority. The 2018

strategy appears more realistic about prioritising defence and resiliency measures within the war fighting force.

- Both strategies highlight the importance of cultivating cyber talent and place significant focus on technological innovation.
- Both strategies recognise the need for alliances and international engagement in order to achieve strategic objectives.

Differences between the two strategies are:-

- Tone of the two documents is strikingly dissimilar. The 2015 strategy strove to "mitigate risk" and "control escalation", whereas the 2018 strategy takes a much more active and risk acceptant tone, pledging to "assertively defend our interests."
- The 2018 strategy exhorts the Defense Department to "win" and "preempt," two words noticeably absent from the earlier strategy.
- The new document articulates a change in the department's cyber mission priorities. In 2015, these priorities included defending the '.mil', preparing to defend the U.S., and "if directed by the President", providing cyber capabilities to support military operations. In contrast, the 2018 document advocates more expansive and active missions to defend forward, compete daily and prepare for war.

The issue here is not whether CYBERCOM should ever have a defence forward mission, but rather what the process might be for deciding to take action under that heading in a particular case. Under the top secret Presidential Policy Directive/PPD-20, a great deal of inter-agency vetting had to take place for out of network operations involving intrusions into systems located in third countries not currently the site of active hostilities. It is reported that President Trump recently removed at least some amount of that vetting. This may result in pushing final decision making down to lower echelons. It is not clear whether General Nakasone, head of CYBERCOM, has sole decision-making authority to conduct operations of this kind. It is not known what the replacement for PPD-20 says about offensive cyber operations, but there are concerns about this process, how intelligence agencies are involved and how the uses of cyber and non cyber power are integrated.

The DoD strategy says that the Department must take action in cyber space during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests. These are:-

- Focus on states that can pose strategic threats to U.S. prosperity and security, particularly China and Russia.
- Conduct of cyber space operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict.
- 'Defence forward' to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of an armed conflict.

- To strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages.
- Collaboration with our inter-agency, industry and international partners to advance our mutual interests.

Cyber Enabled Information Operations

The strategy also alludes to countering adversarial and cyber enabled information operations. Given the emphasis on China and Russia within the strategy, this again helps process a more coherent approach to countering the full range of cyber enabled interference operations instead of viewing computer compromises and disinformation within discrete stovepipes.

The 2018 DoD Cyber Strategy directs the Department to 'defend forward', shape the day-to-day competition and prepare for war by building a more lethal force, expanding alliances and partnerships, reforming the department and cultivating talent while actively competing against competitors. Taken together, these mutually reinforcing activities will enable the department to compete, deter and win in the cyber space domain.

Areas that Deserve More Attention

The relationships the DoD should have with vastly different sectors of critical infrastructure require more attention. How cyber defence is applied at the state and local level and the role the military should play should be debated. Private sector priorities may not always align with government priorities. The private sector, particularly firms that operate globally, have competing interests in maintaining their place in the market. (for example Google's fraught relationship with both the U.S. DoD and China).

The focus on degrading an adversary's cyber capabilities instead of threatening attacks on an adversary's civilian infrastructure looks closer to a counter-intelligence operation rather than a strategic plan to cripple an opposing nation which could be highly escalatory. These kinds of cyber-versus-cyber operations can occur below the threshold of conflict without escalating to conventional military uses of force. But aggressive strategy runs the risk of escalation dynamics. It can never be completely certain that more aggressive strategies in cyber space will not spill over to conventional war fighting domains. More work needs to be done to understand what types of targets or effects might inadvertently trip a country into escalation — something the DoD should continue to explore.

'Defend Forward'

The most discussed term in the Defense Cyber Doctrine is 'defend forward'. It states, "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." The term 'Defend Forward' is mentioned four times throughout the document. The summary does not offer a definition of defending forward. How the Trump Administration will use the newly unleashed offensive cyber capability remains unclear, as the policy's details remain classified. At this

point of time, defend forward is slightly a vague concept and maybe it has been kept that way intentionally. Here the concerns are:-

- An activity outside of American networks.
- Contemplates DoD cyber activities that are not part of an armed conflict.
- Operations that are intended to have a disruptive or even destructive effect on an external network: either the adversary's own system or a midpoint system in a third country that the adversary has employed or is planning to employ for a hostile action.

Ben Buchanan, Assistant Professor at Georgetown University and author of "The Cybersecurity Dilemma", writes:

> "I outlined several cases of the National Security Agency (NSA) undertaking activities that would seem to fit easily under the broad heading of defending forward. In one instance that I recounted at some length, the NSA's intrusion group (then known as Tailored Access Operations) hacked digital infrastructure used by the Third Department of the People's Liberation Army, then made their way upstream and hacked into the computers from which the PLA was conducting their operations. In so doing, the NSA developed an excellent picture of the Chinese operations and used that intelligence to thwart specific Chinese intrusion attempts against U.S. networks. It is probably reasonable to assume that the modern conception of defending forward gives the military authority to conduct similar kinds of operations and perhaps also the ability to interfere directly with adversary operations by manipulating their devices and infrastructure.
>
> This change highlights an important point: the study of escalation in cyber operations is still nascent. My scholarly work has focused on how difficult it is for a nation that suffers an intrusion into a critically important network to interpret the intruders' intent. I argued that it was hard to know if the intruders were setting up for a significant cyber attack or if they were just gathering intelligence. In light of this ambiguity, and due to some particular operational factors endemic to hacking efforts, nations are likely to assume the worst and not give the intruders the benefit of the doubt. It seems reasonable to expect that, as hard as it is to differentiate between intelligence collection and attack in cyber operations, it is even harder still to distinguish between defending forward and attacking forward. If the new strategy permits U.S. operators to be more aggressive than what the NSA was previously doing, that could have significant implications for escalation risks."

Granting defense department officials' the authority to launch retaliatory cyber attacks could risk turning the global internet into a 'free-fire zone', said Martin Libicki, Professor at the U.S. Naval Academy in Annapolis, Maryland, who has written extensively on deterrence in cyber space. Some experts believe there is no revolutionary change to U.S. policy. The U.S. has carried out numerous offensive actions short of declaring war from

time-to time, including in the cyber world. Gary McGraw, Vice President of Security Technology at Synopsys, in reference to the 2010 cyber attack that destroyed nearly 1,000 uranium enrichment centrifuges in Iran and which is widely attributed to the U.S. and Israel, asked "Has everybody already forgotten about Stuxnet?" 'Active defence', or "the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy," was the term frequently used by DoD earlier for navigating the murky space between defence and offence. 'Defend forward' by comparison, can only be construed as active defence plus. It connotes greater geographic latitude with lower limitations on offensive parameters.

Any defend forward operations must be highly targeted with a strong bias for limited to no collateral effects. The U.S. does not want to be responsible for the next 'NotPetya', an attack that started as a targeted Russian operation against Ukraine and quickly ballooned into a global campaign causing shut down of hospitals, massive disruptions to global shipping and commerce, costing billions of dollars in damages. Not only would this outcome hurt America's diplomatic standing, but it would also damage international efforts to establish and enforce norms for behavior in cyber space.

The effectiveness of any defend forward strategy must account for two variables:-

- Duration of denial, disruption or degradation to the adversary's objective;
- Deterrence value.

Cyber attackers distribute their infrastructure across the world in order to preserve anonymity and increase ambiguity. How will the U.S. disrupt or halt malicious cyber activity at its source if the source is located in a country that is friendly or allied with the U.S.? What if the source is located in a country that is adversarial to the U.S.? The former scenario could result in a diplomatic backlash, while the latter could potentially lead to military escalation. There is no easy answer to this problem.

It is also not clear whether 'defend forward' is limited to threats to the government's own networks or it is true for the other privately held networks that the summary confirms DoD will defend.

Takeaways for India

National Cyber Strategy. The National Cyber Security Policy was enunciated in 2013 by Ministry of Communication and Information Technology. As a first document of its kind it has served its purpose. However, in a fast changing dynamic field of cyber it is now time after five years to take a fresh look at the policy and publish a National Cyber Strategy or at least a National Cyber Security Strategy as a large number of countries have already done. It should spell out clear cut responsibilities and specific time lines for agencies responsible for cyber security.

Defence Cyber Strategy. India does not have a National Security Strategy, a National Defence Strategy or a National Military Strategy. Rightly, that has not stopped Headquarters Integrated Defence Staff (IDS) to publish the Joint Doctrine of the Indian

Armed Forces. Similarly, the Joint Doctrine on Cyber Operations, or at least Cyber Defence should be published. Reasonable assumptions can be made.

Responsibility

Command and control structure should be absolutely clear for ensuring the cyber security of the nation. Different agencies have different capabilities. All of these capabilities have got to come under a single authority in times of emergency or a major crisis. Generally, there are three agencies in any country who are responsible for cyber security. These are Law Enforcement Agency, The Department of Homeland Security and The Department of Defense.

Law Enforcement Agency is represented by FBI (U.S.) or equivalent agencies in other countries. Domestic cyber attack and cyber crime investigations are the responsibility of the FBI. Is it the Intelligence Bureau (IB) in India? The IB is mostly involved in counter-intelligence and counter-terrorism activities. There has to be clarity on who is responsible in the cyber field in India.

The Department of Homeland Security in the U.S. and equivalent elsewhere in other countries are the lead for critical infrastructure and defending government computer networks, having primary operational responsibility for the defence of all federal and unclassified civilian networks. In India, somehow the Ministry of Home Affairs (MHA) seems to have washed its hands off on cyber security.

The Department of Defense in the U.S., like India's Ministry of Defence (MoD), is the lead for defending military computer networks, and developing and employing military cyber capabilities.

Normally, responsibility for cyber security of the nation is not entrusted to an intelligence agency. Organisations like The National Security Agency (NSA) of the United States or the Government Communications Headquarters of the United Kingdom (GCHQ) or other such intelligence agencies help others with their expertise in niche technology areas. Responsibilities for cyber defence in India are distributed within the government among several organisations. There has to be coordination and collaboration on cyber issues between agencies and departments. Who coordinates cyber security activities between different ministries? Responsibility and authority must go together. A National Cyber Security Coordinator has no authority over anybody. He draws his strength from his proximity to the National Security Advisor and the Prime Minister's Office. Surely there has to be an institutional mechanism for coordinating such vast and diverse agencies.

Is the Ministry of Communication and Information Technology responsible for the nation's cyber security since the National Cyber Security Policy was promulgated by them?

Security of Government Networks. There should be a centralised authority to secure government networks and the '.gov' domain. Ideally, it should be the MHA. However, in the cyber security field, the Ministry seems to have a miniscule role. The National Technical Research Organisation (NTRO) is a technical intelligence agency that

does not come under any ministry. It works under the National Security Advisor in the Prime Minister's Office. Ideally, an intelligence agency cannot be made responsible for cyber security of a country. They can help other agencies with their superior knowledge and know how in the technology arena.

Cyber Security Audit of MoD Organisations and Defence Industrial Base. Presently, the NTRO does not carry out a cyber security audit of MoD organisations. The armed forces certify themselves for cyber security. Their networks must be audited. If nothing else, the three services should audit their networks with the help of other services. Similarly, Defence Research and Development Organisation (DRDO) networks and organisations, Defence Public Sector Undertakings (DPSUs) and Ordinance Factory Board (OFB) organisations must be audited. Under the 'Make in India' campaign several private sector organisations have become a part of the defence industrial base eco-system handling sensitive equipments and accessories. Their cyber security audit must be carried out by some responsible agency like the NTRO.

Risk Management and Information Technology. Every ministry or department should have a Chief Information Officer (COO) responsible for leveraging technology, cutting down duplication of efforts and utilising information technology funds optimally. They should be accountable for cyber security risk management.

Supply Chain Risk Management. The procurement process must integrate the supply chain risk management process so that networks are made secure and reliable. In the classified and secured Indian Air Force Network (AFNET), there are a large number of network equipments manufactured by the Chinese company Huawei.

Government to Lead Niche Technology Areas. The government should lead in developing and implanting standards and best practice in emerging niche technology areas. Public key cryptography, quantum computing and artificial intelligence are some fields the government should take a lead in terms of research and development.

Space Cyber Security. India is increasingly becoming a space power. There are a lot of vulnerabilities in the space sector. Our space assets and supper infrastructure must be protected from cyber attacks.

Legal Issues. Cyber activities of criminals, state and non-state actors, need to be curbed. Offenders have to be apprehended and prosecuted. Cyber laws and procedures have to be suitably strengthened/amended to combat transnational cyber criminal activities. This should be done in consultation with private industry.

Critical Infrastructure

Role and Responsibilities. Though a lot of work has been done to identify critical information infrastructure and responsibilities for cyber security of respective sectors, a lot still remains to be done. In all such sectors, regulators have to be appointed, and clear-cut responsibilities have to be given. Computer Emergency Response Teams (CERT-In) can issue advisories but cannot enforce implementation. What is the role of

respective ministries must be clearly stated. In the present system, ministries seem to have very limited roles in cyber security.

Exchange of Information. Exchange of information about any breach of security and mitigation measures have to be strengthened between the private and the public sectors. Institutional mechanisms have to be put in place. A trust has to be developed between them. Industry does not trust intelligence agencies easily.

Research and Development. Funds for research and development have to be spent judiciously and prioritised. The private sector must contribute for cyber- related research and development.

The Private Sector

A vast majority of our cyber infrastructure is owned and operated by the private sector like the internet service providers. The government normally would not want to maintain a long term, active presence on private sector networks to provide defensive capabilities. The government, however, should closely work with the private sector in three areas:-

- Setting the conditions for a truly defensible cyber infrastructure.
- Significantly empowering private sector defensive capabilities.
- Providing for interoperable capabilities and joint exercises in the event that a national crisis requires the government to assist the private sector in a more direct manner or to respond directly against a threat to the nation.

Cyber security responsibilities within the private sector are spread over a large area. Coordination and information sharing between these entities is limited and often non-existent. There is a need for an India version of the Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organisations (ISAOs) of the U.S.A. The Government of India should assist the private sector in their cyber security efforts and help facilitate critical cyber security information sharing, both among private sector actors and between the government and the private sector. The National Critical Information Infrastructure Protection Centre (NCIIPC), an organisation created under Sec 70A [1] of the Information Technology Act, 2000 (amended 2008), has taken some welcome steps, introduced standard operating procedures (SOPs) and formats for reporting incidents, but a lot more is required to be done. The private industry must, therefore, come forward for sharing information.

Entities such as Infosys, Tata Consultancy Services (TCS) or Wipro may be aware of a particular vulnerability or threat, and it can take a long time before relevant information spreads throughout the cyber eco-system and results in the deployment of patches, installation of new technologies, changes in network architecture, or the adoption of new policies that adequately counter the threat. Sharing of such information must be done quickly. The government should have programs in place that provide the private sector with threat information data and other forms of assistance designed to help private organisations

enhance their cyber security postures. It is difficult for the private sector to gain access to the wealth of information and assistance that the government, particularly the NTRO and the CERT-In could provide.

Threat information sharing is significantly more efficient when automated, relying on standardised feeds and formats to communicate key pieces of data. The NCIIPC and the CERT-In should continue to encourage automated sharing of threat information and push for greater interoperability between such initiatives, including the incorporation of confidence levels in the sharing of cyber threat indicators (such as IP addresses and MD5 hashes).

The following initiatives are needed:-

- The government should prioritise the identification and sharing of Tactics, Techniques and Procedures (TTPs) as well as exploit targets for sharing with the private sector. This is important as cyber adversaries rapidly vary traditional signatures used to counter cyberattacks, such as IP addresses and MD5 hashes. A greater understanding of the TTPs and exploit targets used by an adversary can allow security professionals to focus on network hardening and detection efforts.
- The government should encourage development of a common language for the exchange of threat information — threat information data is most valuable when all organisations involved use the same terminology to describe various TTPs.
- The government should foster the collection and categorisation of incident data to identify TTPs and other relevant information. A key source of TTP lies in information collected as part of an incident response effort. Thus, there needs to be a greater focus on 'reverse engineering' incidents to identify TTPs utilised and corresponding courses of action that could mitigate such TTPs. Establishment of an organisation like a Cyber Incident and Data Analysis Repository (CIDAR) to define the architecture for an incident repository may be explored. The success of such an initiative will depend on the willingness of organisations to contribute this data.

The American private sector has benefited greatly from the National Institute of Standards and Technology's (NIST's) cyber security framework. This voluntary framework, which consists of standards, guidelines and best practices for organisations to manage cyber security related risk, has been well received in both the private and public sectors. It has helped organisations prioritise and identify areas deserving of additional investment and attention while promoting the protection and resilience of cyber infrastructure across sectors. One can think of having such an organisation in India too.

There is a need to create organisations on the following lines:-

- **U.S. DHS's National Protection and Programs Directorate (NPPD)**. It operates the Cyber Information Sharing and Collaboration Program (CISCP), which can be an invaluable source of threat information data for private entities, potentially providing them with access to government threat information data, including sensitive, classified information. Even in the United States, very few companies are aware of

the CISCP or other assistance programs offered by DHS and other government agencies.

- **Cooperative Research and Development Agreement (CRADA) with DHS.** Once a company is aware of the NPPD program, it must negotiate the agreement. The negotiation of a CRADA, while relatively straight forward, can be confusing to companies unfamiliar with government processes or cooperative agreements and can take months to negotiate. These issues can be resolved in consultation with the private sector.

Conclusion

The recently published U.S. National Cyber Strategy and the U.S. DoD Cyber Strategy are two very important documents regarding the U.S. Government's thinking and policy in the cyber domain. They reiterate the proactive use of offensive cyber capabilities. These amplify the ongoing discourse on the use of offensive capabilities, providing transparency in an area that has for far too long been viewed as a dark art while signaling to attackers that the unfettered deployment of cyber enabled attacks against the U.S. is over. It shows the emergence of a national security framework that acknowledges the realities of a dramatically shifting international system and technological change. It takes a nuanced, multi-faceted approach toward one of the most daunting national security challenges.

India's national security establishments and the armed forces need to read these documents carefully and take appropriate action wherever required to improve India's posture in the cyber domain. Publishing a National Cyber Strategy and Cyber Strategy for the Ministry of Defence may be a good beginning.

End Notes:

1. National Cyber Strategy of the United States of America, September 2018, Available at : https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pd

2. Department of Defense Cyber Strategy 2018, Available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PD

3. Fact Sheet: 2018 DoD Cyber Strategy and Cyber Posture Review, Available at: https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet_for_Strategy_and_CPR_FINAL.pd

4. Kevin Liptak, CNN, John Bolton: US is going on the offensive against cyberattacks, September 20, 2018, Available at: https://edition.cnn.com/2018/09/20/politics/us-cybersecurity-strategy-offense-john-bolton/index.htm

5. Mark Pomerleau, It's a new era for cyber operations, but questions remain, Available at : https://www.fifthdomain.com/dod/2018/09/28/its-a-new-era-for-cyber-operations-but-questions-remain

6. Presidential Policy Directive/PPD-20, Available at: https://fas.org/irp/offdocs/ppd/ppd-20.pd

7. Andrea Little Limbago , The Pentagon Unveils An Aggressive New Cyber Defense Plan, September 21, 2018 Available at : https://taskandpurpose.com/pentagon-cyber-defense-plan

8. Dave Weinstein, The Pentagon's New Cyber Strategy: Defend Forward, September 21, 2018, Available at : https://www.lawfareblog.com/pentagons-new-cyber-strategy-defend-forwar

9. Christopher Painter, The White House Cyber Strategy: Words Must Be Backed By Action, The Strategist, September 25, 2018, Available at : https://www.aspistrategist.org.au/the-white-house-cyber-strategy-words-must-be-backed-by-action

10. Elias Groll , Trump Has a New Weapon to Cause 'the Cyber' Mayhem, September 21, 2018, Available at : https://foreignpolicy.com/2018/09/21/trump-has-a-new-weapon-to-cause-the-cyber-mayhem

11. Derek B. Johnson, Trump's cyber strategy: what they are saying, September 21, 2018, Available at : https://fcw.com/articles/2018/09/21/cyber-strategy-react-johnson.aspx?m=

12. Guest Blogger for Net Politics, The Implications of Defending Forward in the New Pentagon Cyber Strategy, September 25, 2018, available at : https://www.cfr.org/blog/implications-defending-forward-new-pentagon-cyber-strateg

***

(The paper is the author's individual scholastic articulation. The author certifies that the article/paper is original in content, unpublished and it has not been submitted for publication/web upload elsewhere, and that the facts and figures quoted are duly referenced, as needed, and are believed to be correct).

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organisation to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelise fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its inception, VIF has pursued quality research and scholarship and made efforts to highlight issues in governance, and strengthen national security. This is being actualised through numerous activities like seminars, round tables, interactive dialogues, Vimarsh (public discourse), conferences and briefings. The publications of VIF form lasting deliverables of VIF's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

VIVEKANANDA INTERNATIONAL FOUNDATION
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Phone: +91-11-24121764, 24106698
Email: info@vifindia.org, Website: https://www.vifindia.org
Follow us on twitter@vifindia