VIF Paper | September 2021

Deterrence Theory –

Is it Applicable in Cyber Domain?

Maj Gen PK Mallick, VSM (Retd)

Vivekananda International Foundation

Published in 2021 by

Vivekananda International Foundation

3, San Martin Marg | Chanakyapuri | New Delhi - 110021

Tel: 011-24121764 | Fax: 011-66173415

E-mail: info@vifindia.org

Website: www.vifindia.org

ISBN: 978-93-91498-05-4

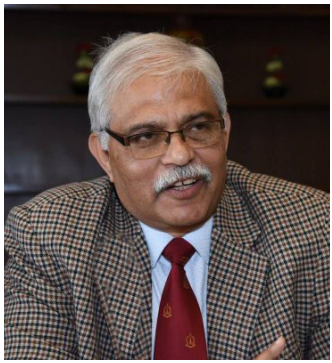
Follow us on

Twitter | @vifindia

Facebook | /vifindia

Disclaimer: 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 The author certifies that the article/paper is original in content, unpublished and it has not been submitted for publication/web upload elsewhere, and that the facts and figures quoted are duly referenced, as needed, and are believed to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.

Cover Image Source : https://www.mindef.gov.sg (Components of Cyber Deterrence)



An Electronics and Telecommunication Engineering graduate from BE College, Shibpore, M Tech from IIT, Kharagpur and M. Phil from Madras University Major General P K Mallick, VSM (Retd) was commissioned in the Corps of Signals of Indian Army. The officer has interest in Cyber Warfare, Electronic Warfare, SIGINT and Technology. His last posting before retirement was Senior Directing Staff (Army) at National Defence College, New Delhi. He runs a popular website on national security issues @ https://www.strategicstudyindia.com. Currently, he is a consultant with Vivekananda International Foundation, New Delhi.

Deterrence Theory – Is it Applicable in Cyber Domain?

"We cannot deter other nations with our cyber weapons. Nor are we likely to be deterred from doing things that might provoke others into making a major cyber attack. Deterrence is only a potential, something that we might create in the mind of possible cyber attackers if (and it is a huge if) we got serious about deploying effective defenses for some key networks. Since we have not even started to do that, deterrence theory plays no significant role in stopping cyber war today." - Richard A. Clarke & Robert Knake, 'Cyber War: The Next Threat to National Security and What to Do About It',2010.

Introduction

The Deterrence Theory was developed in the 1950s, mainly to address new strategic challenges posed by nuclear weapons from the Cold War nuclear scenario. During the Cold War, the U.S. and the Soviet Union adopted a survivable nuclear force to present a 'credible' deterrent that maintained the 'uncertainty' inherent in a strategic balance as understood through the accepted theories of major theorists like Bernard Brodie, Herman Kahn, and Thomas Schelling.[1] Nuclear deterrence was the art of convincing the enemy not to take a specific action by threatening it with an extreme punishment or an unacceptable failure. Nuclear deterrence was assumed to be successful due to the nature of the bipolar world and

the astonishing damage potential of nuclear weapons, which made defence strategies less feasible. However, the United States also sought to deter all major aggression by its adversaries and developed robust conventional military forces to underwrite its conventional deterrence. But transporting the same template to the cyber domain is problematic.[2]

Eventually, deterrence is the manipulation of the cost-benefit analysis an adversary undertakes connected to a given action. A nation can persuade its adversary to avoid taking a specific action by reducing the likely benefits and increasing the potential costs. Cyber deterrence is the manipulation of an opponent's cost-benefit analysis of a given cyber activity.[3] Nuclear deterrence relied on the threat of action. The threat of credible retaliation was enough. The use of nuclear weapons is binary. Either they are used or not. This situation is reversed for cyber deterrence; threat of action is not enough. The offensive cyber operation is not binary, it is reversible and scalable frequently with different consequences. Cyber deterrence policies involve action and retaliation. It may or may not involve the use of military force. Counter-cyber operations, diplomatic, law enforcement, technical and economic penalties are also part of cyber deterrence activities.

Volume, intensity and impact of offensive cyber operations have grown considerably in recent times. Some leading thinkers argue that deterrence will not work in cyberspace. In its current form, cyber deterrence is inadequate. The capacity to confuse attribution, create ambiguity, obfuscate activity and operate undetected makes comprehensive deterrence unworkable. Motivations of cyber actors are different. Criminals do it for money, whereas nation-states pursue national security goals. What deters criminals is different from what deters government agencies. Comprehensive cyber deterrence policy cannot prevent cyber-enabled espionage and offensive cyber operations by nation-states or non-state actors and cybercrime from the Internet.

However, there is another school who think deterrence does work in cyberspace. Nation-states can carry out consistent, destructive actions

in and through the cyberspace. Advanced nation-states with cyber capabilities like U.S., U.K., Russia, China, Israel and Iran can use their offensive cyber warfare capabilities to cause widespread disruption. The U.S. had carried out cyber operations against the Islamic State (ISIS) to disrupt their activities. In December 2015 and December 2016, the Russian government turned off power supply in Ukraine by cyber attacks. If a criminal ransomware attack can shut down a critical infrastructure such as the Colonial Pipeline in the U.S., nation-states can do much more damage. Nuclear weapons were not ever used during the Cold War. Both sides of the Iron Curtain felt that they were unusable. On the other hand, cyber capabilities are used all the time including in disruptive attacks against critical infrastructure. All major powers collect intelligence through cyberspace. Such operations are often the precursor to preparation for cyber attacks.

Various facets of deterrence theory and its applicability in the cyber domain will be discussed in the following Sections:-

Section 1: Definition

Section 2: Characteristics of Cyber Deterrence

Section 3: Attribution

Section 4: Strategy of Cyber Deterrence

Section 5: Cyber Resilience

Section 6: Capabilities Based Deterrence

Section 7: Cross-Domain Deterrence (CDD)

Section 8: Principles of Cyber Deterrence adopted by the U.S.

Section 9: Critical Issues of Cyber Deterrence

Section 10: Chinese Concept of Cyber Deterrence

Section 11: Cyber Deterrence Policy – The Way Ahead

Section 1: Definition

Theorists' Definitions

Karl Mueller defines deterrence as "causing someone not to do something because they expect or fear that they will be worse of if they do it than if they do not." He stresses that deterrence "happens in the mind of the potential aggressor."[4] Richard K. Betts defines deterrence as a strategy for combining two competing goals: countering an enemy and avoiding war. Simply an enemy will not strike if it knows the defender can defeat the attack or can inflict unacceptable damage in retaliation.[5]

The objective of deterrence, as recognised by John Mearsheimer remains the development of fear of the consequences, in particular of military action or a function of costs and risks.[6] Deterrence is a coercive strategy that wants to prevent an actor from taking an unacceptable action.[7] Robert Art defines deterrence as, "the deployment of military power so as to be able to prevent an adversary from doing something that one does not want him to do and that he otherwise might be tempted to do by threatening him with unacceptable punishment if he does it."[8] Joseph Nye defines deterrence as, "dissuading someone from doing something by making them believe the costs to them will exceed their expected benefit."[9] These definitions of deterrence have a common thread: prevent an adversary from taking action to create such high costs for the act that exceed the potential benefits. Robert Art's emphasis is on the military instrument of power, including nuclear weapons as a tool of deterrence, whereas Nye's concept of deterrence infers a broader set of capabilities that could be used to prevent unwanted behaviour.

The U.S. Department of Defense (DoD) Dictionary of Military and Associated Terms, Joint Publication 1-02, defines deterrence as "the

prevention from action by fear of the consequences. . . a state of mind brought about by the existence of a credible threat of unacceptable counteraction." Thomas Schelling, an economist by training, was a master deterrence strategist. His books 'The Strategy of Conflicts' and 'Arms and Influence' are classics in the field. Schelling wrote at a time when debates over nuclear strategy dominated the discussions, even though his work is relevant to all varieties of force application. When discussing deterrence, he stresses the role of threats in his 1960 book 'The Strategy of Conflict', "It is a dozen years since deterrence was articulated as the keystone of our national strategy. . . We have learned that a threat has to be credible to be efficacious."[10] But in his 1966 book, 'Arms and Influence', he defines deterrence more broadly as "to prevent from action by fear of consequences," which opens the behaviour to many causes.[11] Over the past 50 years, scholars have built upon Schelling's work, using it to amplify issues in defence and national security.[12]

Conditions

In order for deterrence to work, at least three conditions must be met:-

- The threat of consequences should be clearly communicated and understood by all parties. This is called 'signaling'.
- Both actors must have as comprehensive information as possible about the capabilities, intentions about their counterparts to be able to rationally assess costs and benefits.
- The threat of punishment must be credible, technically feasible and backed by political resolve.

Attributes of Deterrence

There are seven deterrence attributes which are commonly quoted, These are: *Interest, Deterrent Declaration, Credibility, Fear, Denial Measures, Penalty Measures* and *Cost-Benefit Calculation*.[13]

Deterrence Attributes

Deterrence attribute	Definition
Interest	A state employs a deterrence strategy to protect its interest.
Deterrent declaration	To keep adversaries from attacking the interest, a state makes a deterrent declaration: Do not do this, or else that will happen. This is any adversary action that threatens the interest and that includes either denial measures, penalty measures or both.
Credibility	Credibility is the attacker's calculation of the defender's capability and intent to carry out the deterrent declaration. For other states to take a deterrent declaration seriously, the declaration must be credible and believable.
Fear	If a potential adversary fears the denial the denial of penalty measures, that actor is less likely to take an undesirable action.
Denial measures (passive measures)	Denial is the defensive aspect of deterrence and consists of prevention and futility. Deterrence by prevention means that if an attack is launched, the defensive measures will disrupt the attack to keep it from succeeding. Deterrence by futility means that even if an attack breaches defenses, it will not have its desired effect on the target.
Penalty measures (active measures)	Penalty is the offensive aspect of deterrence and consists of retaliation. Classical deterrence theory demands that penalty measures be certain, severe and immediate.
Cost-benefit calculation	What the benefits and costs of action versus the benefits and costs of restraint?

Similarities between Cyber and Nuclear Deterrence. There are certain similarities between cyber and nuclear conflicts:- [14]

- Both operate at all three level of military operations: strategic, operational and tactical, with the potential to have effects ranging from small to population scale.
- Both have the capacity to create large scale, even existentially, destructive effects.
- Both can be conducted between nation-states, between a nation-state and no-state actors, or between hybrids involving nation-states and non-state actor proxies.
- Both nuclear and cyber conflict "could present the adversary with decisive defeat, negating the need to fight conventional wars."
- Both can intentionally or unintentionally cause cascade effects beyond the scope of the original attack target.

Differences. However, there are some major differences between nuclear and cyber deterrence models. Some of these are:- [15]

- Generally, Nation-states do not take responsibility for offensive cyber operations.
- Examples of Stuxnet attack in Iran or deleting hard drives of Saudi Aramco are not enough to justify claims of awe inspiring and game changing cyber attacks. Neither Iranian nuclear installations nor the Saudi oil company stopped functioning.
- Attribution in cyberspace is extremely difficult unlike identifying a nation-state that can launch a nuclear weapon.
- Nuclear weapons development can be monitored. The development of cyber weapons by nation-states is always under a cloud of secrecy. No international watchdog agency exists to track developments of

cyber weapons.

- Cyber attacks of various types and magnitude are done thousands of times a day. Nuclear attacks cannot be done that way.

Deterrence Challenges. These are listed below:-

- Cyberspace is a domain of constant contact (many actors interacting with unprecedented speed remoteness and speed).
- Attribution of attacks and intrusions is difficult.
- Detection of attacks and intrusions is often delayed.
- Cross-domain deterrence may be escalatory.
- Advanced nations are asymmetrically vulnerable in cyberspace.
- There is a lack of domestic norms and laws for responding to cyber incidents.
- There is a lack of international norms and law for conflict and behaviour in cyberspace.
- The effects of cyber weapons are uncertain.
- Offensive and defensive cyber operations are difficult to distinguish.
- Greater potential for technological surprise that rapidly alters conflict asymmetries.
- Greater tension in the reveal/conceal dilemma (defence is relatively easy).

Section 2: Characteristics of Cyber Deterrence

Deterrence theory in cyberspace differs from classic nuclear deterrence and conventional deterrence in the aspects of actors and means. Cyber deterrence is a result of states' desire to avoid being attacked in or via cyberspace. Potential targets include their military networks, critical infrastructures like finance, industrial sector, communication lines, power grid and transportation. The state also needs to understand the interdependencies of critical infrastructure and the psychological impact an attack could have on the public psyche as indirect impacts of a cyber attack. Defence of cyber elements should not be treated differently to efforts to defend against conventional attacks. The most significant difference when comparing nuclear to cyber deterrence is that the effects of a strike in cyberspace are far from being as absolute as in nuclear warfare.

Joseph Nye states "the term cyber deterrence can be confusing because theorists tend to focus on in-kind or in-domain deterrence rather than on a broad range of tools that can be used both actively and passively and with graduated effects. A response to a cyber attack need not be by cyber means any more than a response to a land attack need be by the army rather than naval or air forces."[16] Richard Clark and Robert Knake argue that "of all the nuclear strategy concepts, deterrence theory is probably the least transferable to cyber war. In the real world, the U.S. probably should be deterred from initiating large scale cyber warfare for fear of the asymmetrical effects that retaliation could have on American networks."[17]

Deterrence in cyberspace is more challenging to achieve than deterrence in conventional domains. Cyber attacks are cheaper to execute compared to the cost of defence of entire networks. The ability to identify the assailant and to view his cyber activity as an act of war, followed by a response

according to the rules of war, is highly challenging. In cyberspace, an attacker has the advantage in that he is to succeed only once. One cannot defend everything. Maintaining and updating defence systems are costly. It is difficult to distinguish between a cyber attack and computer malfunction. Retaliation in cyberspace is difficult to execute because one of the major problems with deterring computer attacks is the difficulty of identifying the attacker in a timely manner. Former Deputy Secretary of Defense of U.S., William Lynn III writes, "Traditional Cold War deterrence models of assured retaliation do not apply to cyberspace, where it is difficult and time-consuming to identify an attack's perpetrator."[18]

Attacks can be masked and routed through multiple computers and networks. Digital forensics can take weeks or months and still may be inconclusive. The technical issues are compounded by the use of proxies by state actors and the frequent overlap between criminal and political actors. This blurring of lines makes it difficult to identify motives and for the defender to identify and hold at risk the resources the attacker values.

Essential Factors for Effective Cyber Deterrence

Execution of cyber deterrence is difficult. There are several factors that should happen to achieve the results of a deterrence strategy. A cyber deterrence strategy should have well-known parameters to operate successfully. Without them, an opponent will not be able to get and understand the defender's intent. It runs the risks of misinterpreting or misunderstanding and increasing the risk of escalation and possibly, a state-on-state confrontation.

Communication. The ability to communicate effectively to the adversaries about the redlines, the crossing of which will invite retaliatory action, is part of any deterrence strategy.[19] While addressing hostile activities in cyberspace, the inability to communicate hinders the ability to send clear messages and deescalate tensions.

Signalling. Signalling is important in international politics specially in the matters of decision to go to war, international economic negotiations, crisis bargaining, regional integration and foreign policies. Signalling is essential for escalation management. Signalling can be done covertly, overtly or through diplomatic, military or economic channels. Signalling, like communication, can be simply ignored, misinterpreted, or not even noticed by the aggressor states.[20] Signalling demands coordinated engagement of various instruments of power. Diplomatic efforts should be seamlessly integrated.

Proportionality. Retaliatory cyber action against a suspected state or non-state actor needs to be proportional. The cyber action by the state should be forceful. At the same time, it should not be so severe that the state gets a negative reaction from the international community. States must consider unintended consequences of a cyber-retaliatory action. In cyberspace, proportionality is difficult to achieve. A nation-state runs the risk of economic or diplomatic blowback for its action. Before taking any kinetic or non-kinetic retaliatory action, factors like promptness of the retaliation, potential political fallout, the projected consequences and battle damage assessment should be considered in the decision-making process.

Attribution. Attribution is an essential component of any deterrence strategy. A defending state has to attribute an aggressor before taking any retaliatory action. A number of problems prevent quick and accurate attribution processes including the time taken to collect and analyse the attack method employed, misattribution and identifying motive and behaviour of actors and outside influences. However, to avoid public embarrassment and reduce the likelihood of collateral damage, an acceptable level of attribution has to be done before starting any retaliatory action. In earlier days, attribution was difficult. But over the past 10 years process of attribution has improved considerably. Prompt, high quality attribution is costly but possible today. As Rid and Buchanan note, "The

larger a government's technical prowess, and the larger the pool of talent and skills at its disposal, the higher will be that state's ability to hide its own covert operations, uncover others, and respond accordingly."[21]

Section 3: Attribution

Attribution is critical for deterrence in cyberspace. Complexities include the time it may take to technically or politically attribute an attack to a specific actor, difficulties raised by false flags, plausible deniability and proxy actors and reliance in some instances on private actors for forensic attribution. Attribution of a cyber attack necessitates time intensive, all source information, often spanning numerous networks and actors.[22]

Factors to be considered in this context are as follows:-

- Reliance on cyberspace is asymmetric. Some states and non-state actors have smaller relative attack surfaces than others, limiting the potential scope and scale of retaliation in kind. Potential adversaries may not be equally vulnerable to cyber attacks
- The difficulty of signalling. It is tricky given the secrecy of cyber operations. Cyber capabilities are less visible than their kinetic counterparts and have limited life spans.
- Retaliation requires proper categorization of an incident and making a proportional response thereafter. In the cyber domain, the purpose and scale of an attack is often ambiguous.
- Difficulty of discerning between offensive and defensive behaviour.
- Deterrence through punishment in cyberspace is nearly impossible. An overwhelming campaign to deliver devastating pain and

suffering on an enemy population is not yet feasible. However, this may change as technology changes.

- Deterrence through denial is difficult due to the perceived ease of offensive operations. Also, there are vulnerabilities an attacker can exploit.

- A multiplicity of actors in cyberspace complicate deterrence. It may not be clear who needs to be deterred and difficult to identify what they value in order to affect their cost-benefit calculus. There is a number of actors actively engaged in this domain, which run the range from nation states to criminal organisations, individual hackers, patriotic groups, private corporations, terrorist organisations etc.

In earlier days, attribution was difficult. But over the past 10 years process of attribution has improved considerably. Prompt, high quality attribution is costly but possible today. As Rid and Buchanan note, "The larger a government's technical prowess, and the larger the pool of talent and skills at its disposal, the higher will be that state's ability to hide its own covert operations, uncover others, and respond accordingly."[23]

Attribution is accomplished through technical network forensics. When an attack occurs, digital footprints can be traced from the scene of the crime. But there are some qualitative difference between:-

- Identifying the machine from which an attack appears to have originated (although it may have been routed through several others on its way to the target),

- Recognising the person behind the keyboard of the actual computer used to launch the attack and the country in which it is located,

- Determining whether a higher authority is responsible for ordering the attack.

A number of innovative techniques have been devised to resolve these differences. Attack indicators can be generally placed in one of three categories:-

- Indicators of Compromise (IOCs): technical details, digital footprints.
- Tactics, Techniques, and Procedures (TTPs). Observations about behaviour consistent with that of known adversaries. This could include whether attack patterns appear to correlate with religious holidays, particular working hours or, in the case of states, foreign policy priorities.
- Human Intelligence.

Cyber forensics use detailed iterated pattern analysis based on TTPs, machine learning algorithms and 'kill chain modelling' to diplomatic indices. Ideally, attribution is based on repeated observation, matching IOCs with TTPs and supplementing with diplomatic factors or human intelligence.

While security researchers are professionals, attribution and decision making may be hindered by cognitive and motivational biases, path dependence or outmoded standard operating procedures, biological factors, emotions and affectations, imperfect information, or stress. Little is known about how these operate in cyber conflict as opposed to conventional conflict, but the shortening of the time horizon, heightened technical complexity and maximisation of the uncertainty condition envisages that sound decision making might actually be more difficult.[24]

Despite the technological advancement attribution still has to contend with the following issues:-

- Attribution remains uncertain due to states' plausible deniability and false flag attacks. The complicity between the attackers and the state is difficult to prove.

- Establishing complicity with a state is a problem. It is feasible to track attackers and their geographic location. It is difficult to establish any formal government role in the cyber attack.

- Attribution can never be certain. Accused states will disagree about their complicity from their government with the attackers. This requires prior intelligence to argue with certainty that the actors were complicit.

Despite the problems of proxies, false flags and the trouble of acquiring high-quality, prompt attribution that would stand up to a court of law, there is adequate attribution to enable deterrence. The following factors become relevant:-

- A defending government will want a relatively high guarantee from its intelligence agencies to avoid escalation by a malicious third party. It can rely on all-source intelligence and network forensics.

- Attacking government or non-state actor knows what it has done, but it cannot be certain about the quality of the opposing forensics and intelligence. It can refute involvement, but it will never know how credible its deception was.

- Attacking government may deliberately leave clues for signalling purposes while maintaining the action of plausible deniability.

- Some organisations or states may have computer systems that are not advanced enough to be harmed by a deterrent attack.

- It is extremely difficult to know if deterrence is working. If no attacks occur, it is difficult to find out why. Maybe the would-be attacker was deterred by the threat of punishment or perhaps the attack failed for some other reason.

When a cyber attack is found out, it is difficult to attribute it to any one particular actor confidently. If the authorities can pinpoint the attacker,

they still must determine whether the cyber attack crossed the retaliation threshold and merits a response. The state should signal that it has the will and ability to respond without giving away too much information about how it would do so. It would allow the attackers to prepare.

Finally, the assumption that all actors in cyberspace including individuals, non-state hacking groups, state intelligence agencies and military operators would act rationally may not be correct.[25]

Section 4: Strategy of Cyber Deterrence

Deterrence

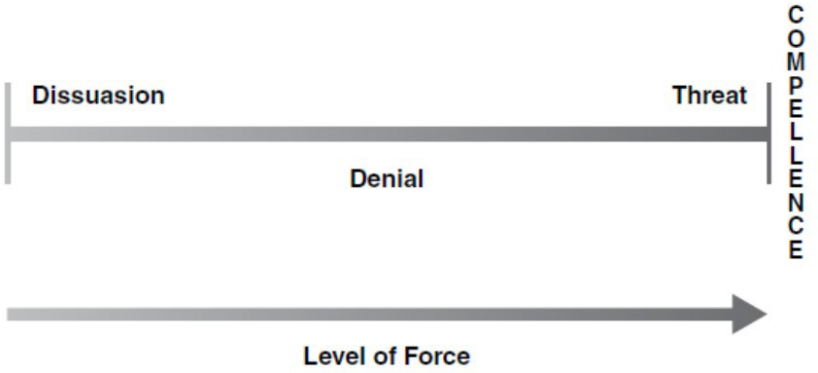
Deterrence is considered as the potential use or threat of punishment to achieve a change in the behaviour of an opponent. Deterrence theory is nothing new but deterring offensive cyber operations is. It identifies two types of deterrence: Deterrence by Punishment and Deterrence by Denial. To function, both these must be credible. A state without nuclear weapons cannot credibly threaten nuclear retaliation. If a state wants to deter, it should provide solid evidence of its capability able to carry out its threat.

Keeping someone from doing something you do not want him to do may be brought about by threatening unacceptable punishment if the action is taken. This is Deterrence by Punishment or Reprisal. In the case of deterring cyber-attacks, deterrence by punishment can be through retaliatory cyber attacks or other means like a kinetic or diplomatic response. It contains an element of coercion. Deterrence by punishment is risky. It can never be known exactly whether it was the threat of punishment that led to the change in adversary behaviour or whether there were other reasons for it. This deterrence will succeed if the opponent believes the threatened costs are sufficiently high and likely to be inflicted.

Convincing the adversary that its objective will be denied if it attacks is Deterrence by Denial. Deterrence by denial is not always successful. This has been demonstrated in the Israel–Hamas conflict. Hamas' use of Katyusha rockets vs Israeli use of Iron Dome batteries shows, after cost-benefit analysis, the cost of deterrence by denial is between 100 to 1 and 200 to 1 in favour of Hamas. In deterrence by denial, there should be a certainty that even in the face of sophisticated cyber threats, the state can ensure resilient networks and systems, maintain robust defences and implement a strong response capability that can project power. Deterrence by denial is usually defensive and not escalatory in nature. Threats of punishment and denial are not exclusive and often reinforce each other.

Dissuasion

Dissuasion is what is actually wanted whether by defence or by deterrence. Deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit. Dissuasion by deterrence operates by scaring a state out of attacking, not because of the difficulty of launching an attack and carrying it home, but because the expected reaction of the attacked will result in one's own severe punishment.



Deterrence can be conceptualised as a continuous spectrum with three components. At one end is deterrence by dissuasion. At the other end is deterrence by threat. In the middle is deterrence by denial. Moving from left to right increases the level of action by the state seeking to deter an adversary. Specific design of a deterrence strategy will depend on the value of the interest at stake and the capabilities of both the actors.[26]

The most passive component of deterrence, deterrence by dissuasion, can take various forms, like efforts to influence target nation public opinion, public diplomacy, or psychological operations, or the offer of a benefit for maintaining the status quo. Dissuasive efforts are notably different from deterrence by threat because they do incorporate the threat of violence or punitive action.

Cyber Deterrence

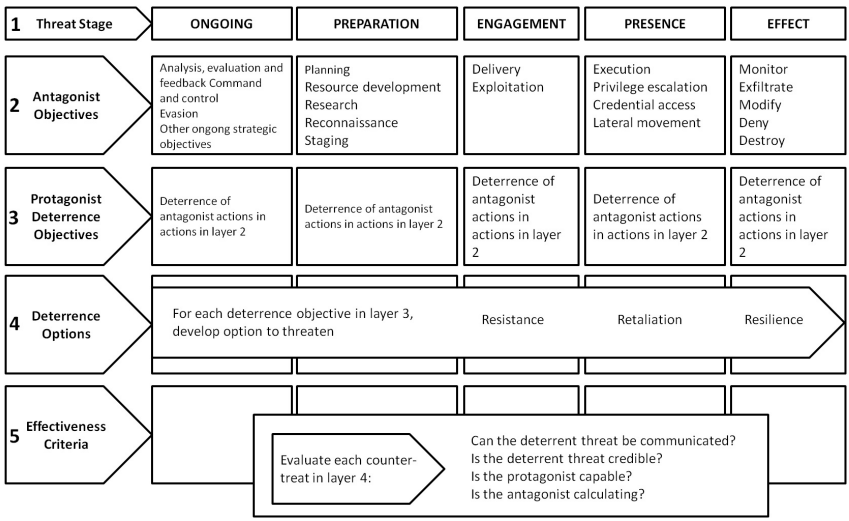
Cyber denial strategies are active in nature. They require continuous revision according to adversary capability development. Static denial strategies in cyberspace will have limited credibility over time. Similarly, punishment strategies also need continuous updating in relation to opposition capabilities and geopolitical concerns. Charles Glaser, recognised four components of basic cyber deterrence:- [27]

- Benefits of taking action. It is harder for the adversary to deter.
- Probability of achieving the benefits. Higher the probability, the harder for the adversary to deter.
- Costs the defender will impose if the adversary takes action. The higher the costs, the more chance the adversary will be deterred.
- Adversary's assessment of the probability that the defender will inflict these costs. The higher the probability, the more likely the adversary will be deterred.

Charles Glaser has identified some problems related to cyber deterrence by punishment:-

- Deterrence relies on the attribution of an adversary's actions.
- Hands-tying and other methods of credibility enhancing measures are lacking in cyberspace. The ability to respond within a domain might not be possible within certain conditions.
- Potential spillovers in which limited within domain operations result in cross-domain, kinetic responses. As of now, there is limited evidence of cross-domain responses. Cross-domain retaliation changes the escalation framework from digital to kinetic or others. It poses a challenge for states wanting to establish credibility while controlling the potential escalatory ladder.
- Most valuable assets in cyberspace may not be destroyed or degraded. It can be stolen and used.

Cyber Deterrence Framework



Source : Eva Uribe, and Michael Minner, Cyber Deterrence and Resilience Strategic Initiative: Intern Briefing available at: https://www.osti.gov/servlets/purl/1806268

Means of Deterrence and Dissuasion

Cyber deterrence is part of general deterrence acts; that is also at the heart of the U.S.' mixed cyber and kinetic response strategy.[28] There are four major mechanisms to prevent and reduce adverse actions in cyberspace: threat of punishment, denial by defence, entanglement and normative taboos.

Punishment. Retaliatory threats of punishment are not likely to be effective in the cyberspace. Here the identity of the attacker is unclear. What assets can be held at risk and for how long is not known. However, punishment remains a crucial part of the dissuasion equation in cyberspace.

Denial. Cyber defences are generally porous. The conventional perception is offence dominates defence. However, strong cyber defences can build resilience or the capacity to recover. Resilience is required to reduce an adversary's advantages of attacking critical infrastructure. It gives an option of using cyber and non- cyber means for retaliation. Investments in resilience can improve deterrence in cyberspace. Attackers have limited resources and time. By reducing the attacker's resources and time, a potential target interrupts the cost-benefit model that creates an incentive for attack.[29]

Entanglement. It is an important means of making an actor perceive that the costs of a cyber attack will exceed the benefits. Entanglement refers to the presence of several inter-dependences that make a successful attack concurrently impose severe costs on the attacker and the victim. A potential foe may not attack if there are benefits of the status quo. In a scenario that visualise a Chinese cyber attack on the U.S. power grid causing financial loss on the U.S. economy, the two countries' economic inter-dependence would lead to monetary loss to China as well. Growing importance of the Internet to economic growth may increase broad incentives for self-restraint.[30] However, entanglement might not produce substantial costs for a state like North Korea, which has a low level of

interdependence with the international economic system.

Norms. Norms can inflict costs on an attacker even if the attack is not repulsed by defence and there is no retaliation. Normative considerations can discourage actions by imposing reputational costs that can harm an actor's soft power.

Whatever be the case, some amount of attribution is needed for norms to work. The difference between a computer program which is a cyber weapon and a non-weapon may be a single line of code. The same program can be used for genuine or malicious purposes depending on the intent of the user. Cyber arms control cannot be like the nuclear arms control of the Cold War. Confirmation of the absence of cyber weapons is practically impossible.

Deterrence Mechanisms

Breakdown of various deterrence mechanisms by time of cost imposition or denial of benefits relative to the attack phase is as follows:-

DENIAL	ENTANGLE-MENT	NORMS	CYBER PER-SISTENCE	PUNISH-MENT
Antagonist is dissuaded from action; pe ceived benefits of action reduced or eliminated	Simultaneous costs to both protagonist and antago-nist due to interdepen-dencies	Damage to antagonist's reputation is perceived to outweigh benefits	Through threats and regular use of force, antago-nist establishes norms and conditions that reduce incen-tives	Prevent-ing an action by fear of the conse-quences

Source : Eva Uribe and Michael Minner, Cyber Deterrence and Resilience Strategic Initiative: Intern Briefing available at: https://www.osti.gov/servlets/purl/1806268

None of these above mechanisms of deterrence and dissuasion is perfect. However, a combination of these shows the kind of means by which it is possible to reduce the possibility of adverse acts in the cyber domain. These can be complementary to each other. There is also a component

of learning involved as organisations and states develop a more refined understanding of the costs of cyber warfare and the growth of their economic dependence on the Internet. The policy that focuses solely on punishment may miss some important political behaviour that shows that dissuasion and deterrence and are working in the cyber realm despite the problem of attribution.

The How, Who and What of Cyber Deterrence and Dissuasion

How	Punishment	Denial/Defence	Entanglement	Norms/ Taboos
Who	Both state and non-state actors	Small states and non-states, but not advanced persistent threats	Major states such as China; less so North Korea	Major states; less to rogues; some non-states
What	Major use of force; sanctions against sub-LOAC levels of activity	Some crime and hacking; imperfect against advances states	Major use of force; major sub-LOAC actions	LOAC if use of force; taboo on use against civilians; norms against cybercrime

Note: LOAC stands for laws of armed conflict.

Cyber Coercion

Compared to deterrence, coercion is about getting the opponent to do something he does not want to do, or making him halt an action you do not want him to take. It involves a change in the status quo and the adversary must change his behaviour. It is harder to coerce than to deter. Unlike deterrence, the targets of coercion are likely to value the issue at stake more highly. The coercer needs superior and diverse military capabilities.

Offensive Cyber Operation is likely to be one of the essential tools of statecraft. Cyber threats can compel targets to doubt their ability to wage

information warfare successfully because of the apparent threat of the coercer's capabilities. Threats inject fear and doubt into the performance and security of a network and then the thought of an adversary in a nation's networks could be exploited for a coercive purpose. There is a need to develop a better understanding of how cyber coercion might emerge, build systems to provide warning of impending operations and make strategies to deter and respond.

Coercion Operations. Cyber operations intended to coerce are a small part of overall cyber operations globally. Espionage remains the main purpose of states' cyber operations. Cyber coercion efforts of some countries are given below:-

- Russian cyber operations show some coercive intent in Ukraine and Montenegro.
- Chinese cyber operations show a continued focus on espionage, but potentially with some coercive intent as a secondary objective.
- Iranian cyber operations appear more focused on retaliating against regional neighbours and the West.
- North Korea has routinely engaged in coercive acts in the physical world and sees cyber operations as another means to coerce others.

Assessment of these cases indicates how the threat, threat actor and the desired change in behaviour are often unclear or ambiguous. However, this ambiguity does not appear to prevent countries from pursuing these coercive campaigns.[31]

Counter Argument and Response to Cyber Coercion. Offensive cyber operations can spill over onto the general internet. Code can be reverse engineered to work against the attacker's own poorly defended networks. Attacks may not be able to locate their targets as assumed vulnerabilities could be patched. Defensive measures like passwords, encryption, loggers and access controls make the attacker's task difficult. It is difficult to predict

how an attack might behave in the target environment. New software and new cyber weapons both have high error rates and low reliability.

Expectedly, some countries are constrained by legal norms than others. Less powerful countries will be more interested in upsetting the status quo. They will try to capitalise on a means of attack that the more powerful is quite vulnerable against.

Compellence [32]

In case deterrence fails, reversing the new status quo may require applying punitive measures against the target. This strategy is called 'Compellence'. It attempts to force a return to the previous status quo. If effective, the credibility of future deterrence may increase. Thus, deterrence and compellence can work as a feedback loop where the effectiveness of one increases or decreases the need and effectiveness of the other.

Thomas Schelling explained two forms of coercion: active coercion (compellence) and passive coercion (deterrence). [33] The former involves the active use of force in some way to compel action by another, whereas the latter involves the threatened use of force to either motivate action or refrain from a particular action. The distinction is more of a continuum. Some states may combine compellence actions with the threat of more devastating consequences to accomplish their ends.[34]

Compellence is "A threat intended to make an adversary do something. In deterrence, the punishment will be imposed if the adversary acts; in compellence, the punishment is usually imposed until the adversary acts. The central characteristic of both forms of coercion is that they depend, ultimately, on cooperation by the party receiving the threat. This is by no means friendly cooperation, but it is cooperation nonetheless." Compellence is the more complicated form of coercion since it requires precise signalling and communication through threats and acts. It is more dependent than deterrence on an accurate assessment of enemy will. A coercer seeking to compel must make clear what it wants the target

state to do, including 'how much' and for 'how long'. The coercer must be prepared to climb the ladder of escalation if the target state resists the coercer's demands. The armed forces have many powerful tools to employ for compellence, including air, sea, land and cyber power. Compellence is often combined with diplomacy and these instances are usually referred to as 'coercive diplomacy'.

Offensive cyber operations can alter how states use their military power. The effects of offensive cyber operations do not necessarily have to be exposed publicly. The compelled party can back down post-action without losing face, thus de-escalating the conflict. Deterrence and compellence can be used both by small states and large states. It is an actor's will and determination rather than its raw power to defend in physical, military or economic terms that usually dictates the outcome in a coercive interaction.

Cyber Defence

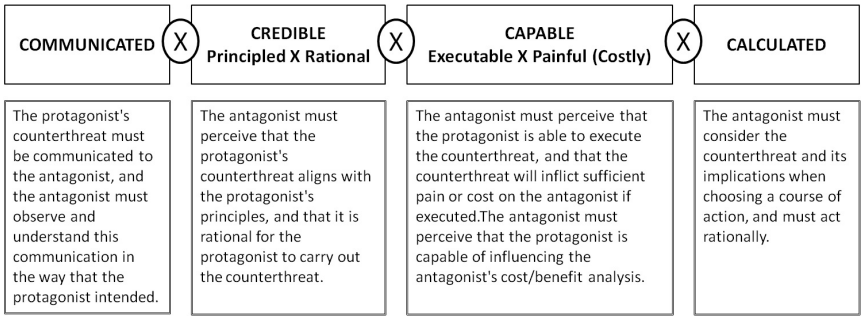
Significance of cyber defence can never be underestimated. Best practices for cyber security are promulgated and updated by government agencies and IT companies regularly. These are readily available and easy to implement. The problem is how to improve cyber defences at scale. The government has to work closely with large technology companies to implement cyber security measures for everyday Internet use.

A robust defensive capability is a deterrence. It makes the attacker to believe that it is not meaningful for him to spend in an attack as his chances of breaking through the defence system are small. The attacker is not certain whether the information he steals is reliable or false information.

In the cyber domain states have to be resilient. If the adversaries know that the digital infrastructure is resilient, there is a credible threat detection and prevention system and there is a capability to carry out counterattacks, the deterrence becomes much more credible.

What makes Deterrence Counter-Threats Effective?

A distillation of deterrence theory literature shows how deterrence counterthreats fail. An effective deterrence counterthreat must have all of the following components:-



Source : Eva Uribe and Michael Minner, Cyber Deterrence and Resilience Strategic Initiative: Intern Briefing available at: https://www.osti.gov/servlets/purl/1806268

Section 5: Cyber Resilience

Purpose of Cyber Resilience

The U.S. Defense Science Board Taskforce on Cyber Deterrence, 2017, stated that "Unfortunate reality is that, for at least the coming five to ten years, the offensive cyber capabilities of our most capable potential adversaries are likely to far exceed the United States' ability to defend and adequately strengthen the resilience of its critical infrastructures." In the cyber domain, resilience as a means of deterrence is crucial because adversaries are not waging direct cyberwar; they are using cyber methods to produce effects below the threshold of armed conflict. Cyber resilience helps to resist attacks, limiting effects and recovering swiftly once attacked.

Resilience exists independently of deterrence. But, resiliency principles are compatible with fundamental deterrence concepts. By denying the

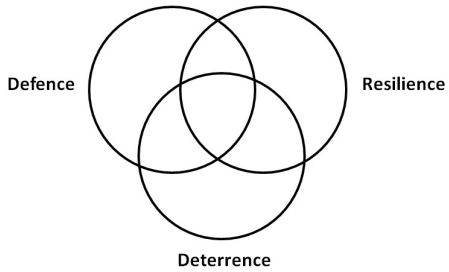
benefits of an attack through defensive measures or resilience, a defender increases the attacker's costs. Key cyber resilience concepts include:-

- Have systems in place that minimise the consequences or impact of an attack.
- Sustain operations throughout and after an attack.
- Recover and adapt to new conditions after an attack.

To deter potential attackers, these three system attributes must be signalled to the attacker to perceive fewer gains and a need to expend more resources to achieve the desired effect.

Resilience is defined in the U.S.' Presidential Policy Directive -21 (PPD-21), as "the ability to prepare for and adapt to changing conditions and withstand and recovery rapidly from disruptions."[35] The Cyber Deterrence and Resilience Strategic Initiative (CDRSI) defines resilience as having systems in place that minimise the consequences or impact of an attack, that sustain operations throughout and after an attack, and that recover and adapt to new conditions after an attack has occurred.

Resilience and deterrence are both part of a comprehensive cyber strategy where tactics may overlap across defence, resilience, deterrence and other strategic spaces. Notional Components of a Comprehensive Cyber Strategy are:-

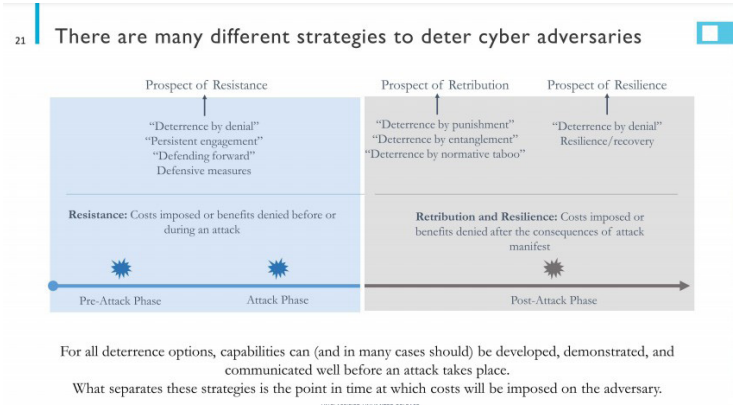


Source: Ann E. Hammer, Trisha H. Miller, Eva C. Uribe, Cyber Resilience as a Deterrence Strategy, Sandia National Laboratories, September 2020

Some of the methods to improve resilience could be as follows:-

- New communications architectures include redundancies through multiple media: cable landlines and fibre optical cables, mobile networks, backup and relay stations, use of UAV to relay communications and space communications.
- Behavioural and doctrinal innovations to reduce reliance on always-on connectivity. As a part of professional military education, how to respond to communication disruption and internet outages should be taught.
- Armed forces should operate without taken for granted communications and use alternative means for distributing public information.
- Consider serious physical and cyber attacks on critical infrastructure, especially communication infrastructures.
- Harden satellites against directed energy attacks, cyber-attacks and anti-satellite weapons to address space vulnerabilities

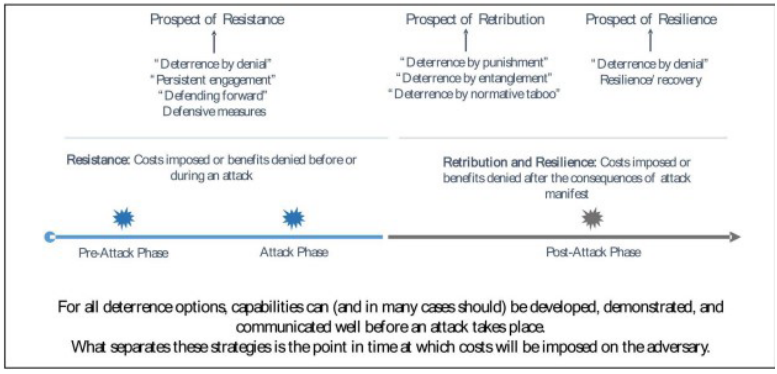
There are many different strategies to deter cyber adversaries as shown below:-



Source : Eva Uribe and Michael Minner, Cyber Deterrence and Resilience Strategic Initiative: Intern Briefing available at: https://www.osti.gov/servlets/purl/1806268

Cyber Resilience in Deterrence

The objective of resilience is to survive and overcome an attack and by preparing, withstanding, absorbing, adapting and recovering from an attack. Deterrence by resilience influences the perceptions of potential adversaries. It involves a defender threatening to impose costs and deny benefits to an attacker. Breakdown of various deterrence mechanisms by time of cost imposition or denial of benefits relative to the attack phase is shown below.



Source: Ann E. Hammer et al., Cyber Resilience as a Deterrence Strategy, Sandia National Laboratories, September 2020 available at: https://www.osti.gov/servlets/purl/1668133

The attacker must be made to perceive the defender's resilience along the following lines:-

- Being sufficiently communicated and credible;
- Defender's credibility in conducting and sustaining this added imposition of cost;
- Re-calculation of the perceived changes in his costs and benefits;
- His ability to adjust his actions according to these changes.

Without these four criteria being met (the '4C'), resilience measures will not succeed. The 4C's that relate precisely to deterrence through resilience

is shown in Figure below.

The 4C's of Deterrence through Resilience

Communication	The attacker has previously observed the defender demonstrate that the effects of similar attacks have been mitigated or that the defender has been able to recover promptly.
Credible	Attacker perceives that the defender believes resilience measures are in its own best interest to create and implement (e.g., not too expensive), also that the resilience measures are consistent with the defender's principles (e.g., do not violate certain rights/freedoms).
Capable	Attacker has sufficient visibility into the defender's resilience to believe their attack would be ineffective as well as that it would require too many resources to overcome the defender's resilience measures. The attacker believes the defender has the ability to sustain resiliency across all relevant systems.
Communicated	The attacker has previously observed the defender demonstrate that the effects of similar attacks have been mitigated or that the defender has been able to recover promptly.
Calculated	Attacker perceives that the defender believes the attacker is a rational actor and has sufficient information about the attacker's interest to influence decisions.

Source: Ann E. Hammer et al., Resilient Energy Systems and Cyber Deterrence and Resilience Strategic Initiatives, Sandia National Laboratories, September 2020 available at: https://www.osti.gov/servlets/purl/1668133

There is no cyber deterrence strategy that is perfect. Certain scholars question whether cyber deterrence is possible.[36] The cyber domain has various exclusive challenges. The following table illustrates the role of deterrence by denial in the cyber domain, often achieved through cyber resilience.

Deterrence of Denial by Resilience in the Cyber Domain

Unique Cyber Domain Challenge	Role of Deterrence/Resilience
Wide range of attacker capabilities, cost/benefit structures and level of risk adversity.	• Implementing and constantly evolving the environment leads to the principle motive of denial which is to make it more difficult and/or require more resources to achieve the goal. • The ability to manipulate cyberspace in the favour of the defender makes it difficult for the attackers to obtain the full potential payoff; few other applications favour the defender as cyberspace deterrence does.
• Attribution is difficult because of the wide range of potential threat actors as well as the use of third-party and proxy to disguise attack origins.	• An unknown attacker may be deterred by denial; building cyber resilience through passive denial defences (e.g. hardening systems) may make the attack less attractive even if identity is not fully known. • Ensuring a well-protected target and/or the ability to recover quickly (via redundancy and resiliency) influences the cost/benefit ratio, regardless of the ability to attribute (Nye, 2011).
• Cyberspace is a unique operational domain where military operations cannot be separated from civilian functions (i.e., business, criminal, social).	• Deterrence must apply to both virtual and physical aspects of the domain. • Denial tactics that build defensive stability in the environment may be an effective deterrence strategy that avoids disproportionately affecting legitimate, non military operations in cyberspace. • Retaliation and escalation tactics do not work well in cyberspace; however, denial strategies (i.e., demonstrating resilient systems) can be effective by influencing adversary decisions and mode of operation.

Source: Ann E. Hammer et al., Cyber Resilience as a Deterrence Strategy, Sandia National Laboratories, September 2020 available at: https://www.osti.gov/servlets/purl/1668133

Section 6: Capabilities Based Deterrence

Indication of Cyber Capabilities

In recent times, Michael Fischerkeller and Richard Harknett have argued convincingly that deterrence is the wrong model. They recommend strongly a "capabilities-based strategy that would focus less on who might threaten the United States or where it might be threatened, and more on what the United States wants to be able to do in cyberspace."[37] For deterrence to be powerfully capabilities based, it must be:-

- Rooted in cyber operational capabilities;
- Separate from any specific red line;
- Known by or communicated to adversaries;
- Planned to cause restraint in adversaries.

None would claim that deterrence can be accomplished based on these four points. But these can help in thinking about how capabilities affect deterrence. Capabilities-based deterrence is likely to succeed when it is tailored and targeted. The U.S. Defence Science Board concludes that "The U.S. cyber deterrence posture must be 'tailored' to cope with the range of potential attacks that could be conducted by each potential adversary."[38] The advocates of cyber deterrence argue for tailoring, denial and layering.[39] The aim is not to stop all attacks but to reduce their intensity and prevent certain typical cyber operations. These ideas have led to several overlapping archetypes of deterrence – 'A loud shout', 'A loud organisation', 'A quiet threat' and 'A symmetric counter'.

A Loud Shout. It is achieved by flaunting a cyber capability to scare current and potential adversaries. To show firmness and ability to punish, a

nation might shut off the street lights in an opponent's capital or interrupt a water treatment plant or the nation's internet backbone. It should be loud and clear that it was a deliberate event and worse could happen if the issue at hand is not settled satisfactorily. Stuxnet showed the capability not just to a particular country but to all who were paying attention. A loud shout in cyberspace is challenging, since it amounts to revealing own cyber capability. In cyberspace it has been considered problematic since revealing a cyber capability provides the target with suggestions for how to defeat it.

A Quiet Threat. A quiet threat may be made explicitly or subtly flaunted so that opponents know something they value is at risk. The Russian intrusions into U.S. electrical grids is an example. A quiet threat may be based on an earlier successful cyber attack. It can be visualised the Chinese quietly threatening U.S. policymakers with a mass or selective release of personal information from the OPM data breaches.

A Symmetric Counter. It is a capability developed to counter a similar capability suspected to be part of the resource of the adversary state. If a state finds another is conducting intrusions into its electrical grid, then developing similar capabilities against the opponent's grid would be a type of capability-based deterrence if properly signalled to the other side.

A state's cyber capabilities can lead to restraint on the part of the opponent state. But there is no substantial evidence to show that a policy stance of having strong cyber capabilities deters adversary nation-states. There is a counterargument - capabilities beget capabilities, operations beget operations. There is ample evidence to show that the Iranians, Chinese and Russians understood the U.S. cyber organisations, capabilities and operations. Given the low cost of developing cyber capabilities, a number of countries have joined the fray.

Though it is commonly believed that using a capability means that it cannot be used again, such argument against capabilities-based deterrence

may not necessarily be valid. More often than not, vulnerabilities remain unfixed by busy cyber defenders. The Russian malware Black Energy and Havex, inserted in Western energy grids were active for several years and remained effective. The Russians did not display their capabilities openly. They were not deployed as part of a deliberate operation to deliver a deterrence threat. This capability was not known to the U.S. decision-makers. Russians planted the malware in some of the most sensitive American critical infrastructure networks. This made the impending threat imminent. The message to the Americans was clear: If the U.S. doesn't calibrate their response option correctly, the impact could be felt immediately in specific plants in the electrical grid. This message was understood by the defender's, *i.e*. American decision-makers, and included in their calculus.

If capabilities-based deterrence depends on the clandestine implantation of weapons that can be detonated remotely, it may lead to escalation and miscalculation. Things happen in the cyber domain at the speed of light.

Not Deterrence but Tit-for-Tat

The U.S. has spent billions of dollars to develop cyber organisations and capabilities, enough to intimidate adversaries. Traditional cyber deterrence seems to be more effective. The logic of difficulty to attribute cyber attacks does not hold good. Neither Iran nor the U.S. had any doubt about who its adversary was.

Nuclear weapons were never used during the Cold War. In comparison, cyber capabilities are used regularly, including disrupting attacks against critical infrastructure. All major nations collect intelligence through cyberspace. It is difficult to distinguish between intelligence collection operations and preparation for cyber attacks. Edward Snowden has revealed that the U.S. possesses and uses such capabilities with greater frequency and skill than anyone else in the world. In cyberspace, Russia, China, and Iran have reasons to feel that they are the aggrieved party.

Section 7: Cross-Domain Deterrence (CDD)

The Concept

For a long time, scholars in the West feel that the concept of deterrence is too big to be kept in a single domain; particularly in the context of cyber deterrence, where it requires a comprehensive mix of military, economic, diplomatic and legal measures coordinated within an overall deterrence posture.

States interact in a variety of domains. Not all of them are military in nature. Traditional concepts of nuclear and conventional deterrence developed and implemented during the Cold War are no longer valid in today's strategic environment. The U.S. National Security Strategy of 2017 states, "deterrence today is significantly more complex to achieve than during the Cold War. Adversaries studied the American way of war and began investing in capabilities that targeted our strengths and sought to exploit perceived weaknesses." State and non-state actors have started using a wide range of coercive tools to hurt adversaries against the background of various technological, economic, social and geopolitical macro trends. These made new forms of power and influence projection across different domains possible.

Today, interstate wars are extremely costly. Major military powers are not inclined to wage wars against each other. To achieve their political objectives, they try and find alternative ways. The emerging hybrid or grey zone warfare concepts are the simultaneous employment of military and non-military instruments below the conventional military threshold aiming to exploit adversary's vulnerabilities in the pursuit of political objectives. Innovative actors have been using these avenues strategically to considerable effect.

These developments have led scholars to think about cross-domain deterrence in dealing with adversaries employing cross-domain strategies. Cross-domain deterrence involves the use of threats in one domain to deter activities in another domain. It is the probability of retaliation from one domain to another which constitutes the essence of CDD.

The concept of CDD has been developing over the past few years. A recently published edited volume of Jon Lindsay and Erik Gartzke on cross-domain deterrence, with a Section on cyber deterrence, the scholars write, "cross-domain deterrence is not new today, but its relevance is increasing. Strategic actors have long combined capabilities or shifted domains to make coercive threats or design around them […] As a larger and more diverse portfolio of tools available for coercion complicates strategic choices, a better understanding of cross-domain deterrence becomes a critical asset for effective national security strategising."[40]

The Clausewitzian formula that war as politics by other means is inherently cross-domain. The precise nature of 'other means' is important. Today several different military and non-military means are available. Scholars point out that "Clausewitzian conditions of fog and friction . . . are likely to become ubiquitous as cross-domain technological complexity increases."

Definition

In the 2019 volume 'Cross-Domain Deterrence: Strategy in an Era of Complexity', Erik Gartzke and Jon R. Lindsay define CDD as "the use of threats in one domain, or some combination of different threats, to prevent actions in another domain that would change the status quo. "[41] Dawkins defines it as "the ability for the weapons or tools of power from one domain to be used to deter the weapons or tools of power in another domain. "[42] Mallory defines successful cross-domain deterrence as a state, "when an opponent has no incentive to initiate or escalate conflict at any given intervention or escalation threshold in any given domain of warfare—both vertically and horizontally within that domain

and laterally into one or more additional domains of warfare.[43]" Mallory asserts that "because war in space and cyberspace cannot be limited to the boundaries of a single geographic theatre of military operations, military leaders and analysts have increasingly chosen to highlight the need to deter potential adversary aggression within and across all five domains of military activity."

CDD involves actions on land, sea, air, space and cyberspace, and sanctions and other non-violent instruments. CDD is about preventing escalation in any domain and across them. The threat of employing non-cyber kinetic capabilities to deter unwanted behaviour in cyberspace is CDD. May 2019 Israeli air strikes at a building housing cyber hackers from Hamas can be seen as an example of cross-domain retaliation.[44]

CDD in Today's Warfare

Currently, warfare raises two major issues. There is advanced integration and synchronisation of military operations across land, air, sea, cyber, and space domains. Also there exists inherent disharmony between strategic, operational and tactical levels of war. Concepts of multi-domain operations or all-domain operations are being developed to synchronise actions both horizontally across domains and vertically across levels of war. Because of the cross-domain nature of the challenge, strategists are looking at similar responses, including CDD. In this new background, cyberspace is a decisive arena in broader great power competition (GPC), with significant implications for CDD.

CDD has problems with the credibility of threats, proportionality and the complexity of signalling and escalation control. The essential issue with CDD is the challenge of making the retaliatory threat credible in the challenger's eyes.[45] There is some contrary aspect of CDD, *viz*, threats in the cyber domain can generate instability and risk for deterrence across the domains. Offensive cyber actions that target a state's nuclear command, control, and communications could weaken strategic deterrence and

increase the risk of war.[46]

Signalling in the cross-domain context is a complex affair. It is difficult to relate signals about specific actions in one domain to anticipated reactions in another domain. Signalling in cyberspace is difficult as the relevant infrastructure of the cyber domain is not under the government's exclusive control. Signals may get lost or be ignored by the adversaries. On the other hand, it can be argued that cyber weapons possess signalling advantages compared to traditional instruments. These can be used as a show of force without starting the conflict because they do not always involve violent, kinetic effects. It may be sufficient to signal intent even though avoiding escalation.[47]

The nature of the cyber and space domains and the character of technologies used in these domains can produce escalation risks. Cyber and space domains can become unstable and can spread effects to other domains in CDD. From the space deterrence perspective, some experts gave the idea of 'layered deterrence'. It includes a concurrent combination of international norms, retaliation, entanglement and denial of benefit, which can be conducted across domains.

Development of CDD

China. It is generally felt that Russia and China and have developed CDD concepts. Chase and Chan in 'China's Evolving Approach to 'Integrated Strategic Deterrence' argue that Chinese understanding of CDD includes "a multidimensional set of military and non-military capabilities that combine to constitute the integrated strategic deterrence posture required to protect Chinese national security interests."[48]

Russia. Adamsky argues that the Russian theory of CDD and compellence is inherently intertwined, is still evolving and is being tested in the contemporary strategic practice.[49] He views Russian CDD as being composed of three intertwined concepts: traditional nuclear deterrence, non-nuclear (conventional) deterrence relying primarily on

precision-guided missiles and special forces, and informational deterrence in cyberspace. In practice, this results in "uninterrupted informational deterrence waged on all possible fronts against all possible audiences, augmented by nuclear signalling, and supplemented by intra-war coercion."

Problem Areas. The domains and the forces which can be employed in each of them are so dissimilar that their synergistic use proves to be very complex, as both military and foreign policy practitioners have experienced in recent years. During the Obama administration, the U.S. Government grappled with devising a suitable response to Russian intrusion in the country's elections.[50] European governments experienced similar challenges as they were not prepared to communicate responses to Russian disinformation campaigns.[51]

Shawn Brimley argues that, "cross-domain deterrence dynamics will constitute a core analytic issue for the U.S. defence, diplomatic and intelligence community, particularly as shifts in the actual or perceived balance of power in the sea, air, space, and cyberspace become more opaque."[52] Juarez recommends that successful CDD can include some combination of five distinct strategies: counter-force (attacking the types of assets that launch the attack), counter-value (attacking high-value targets of the opponent), tit-for-tat (attacking a target of similar value), denial (denying the opponent's attack), and ambiguity (being ambiguous about one's response).[53]

CDD and Cyber Domain

There is a close conceptual and historical relationship between CDD and cyber security. Cyber capabilities provide command and control and intelligence in and across all other domains. James Lewis argues that "deterrence in space or cyberspace cannot be domain limited. It will require threats in other domains, such as saying that an attack on our satellites could lead to an attack on terrestrial targets."[54]

According to Schneider, "It is the difficulty of deterring cyber operations that have provided the catalyst for discussion about the role of cross-domain deterrence as a substitute for within-domain deterrence strategies…… The resounding theme in the current debates about deterrence in and through cyberspace is the role that uncertainty will play in successful cyber deterrence, uncertainty about effects of cyber attacks, capabilities to create cyber attacks, actors conducting attacks, and responses to cyber attacks. The uncertainty is a technical characteristic of these operations but extends to the behavioural reaction to cyber operations."[55]

However, cross-domain retribution for cyberspace deterrence invokes a very important concern about proportionality. In 2014, when the Sony cyber attacks were attributed to North Korea, President Obama promised to "respond proportionally" at a time and place of his choosing. The most apparent proportional response is an attack in kind on an adversary's cyber infrastructure. Here, North Korea had no equivalent private corporate target like Sony. Shortly after the attacks, Obama signed the executive order allowing for sanctions against cyberspace attacks. The Obama administration felt that economic sanctions were appropriate proportional punishment options for many types of cyberspace attacks.

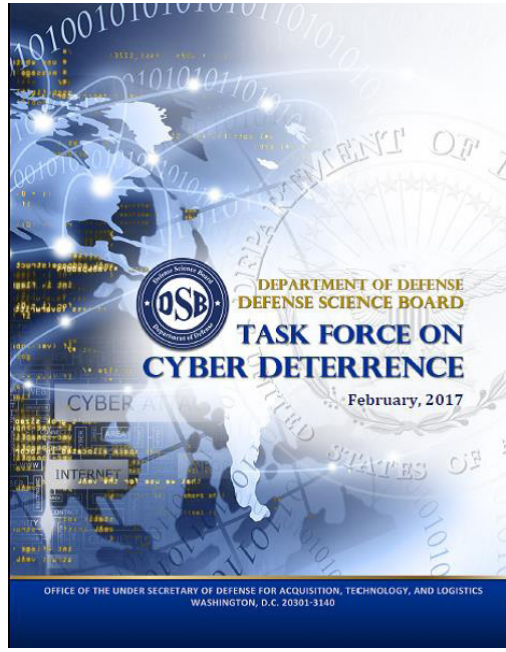
The following questions arise:

- If a cyber attack causes a financial institution to lose resources, what are the most appropriate non-cyber proportional responses?
- If a cyber attack takes out a command and control node, would a kinetic attack like a bomb be considered proportional?[56]
- There are significant cognitive differences between the virtual effects of cyberspace attacks and the solidity of a similar physical attack that damages life or limb.
- A question cames up as to how to deter terrorists.

Section 8: Principles of Cyber Deterrence adopted by the U.S.

Report of the U.S. Defense Science Board (DSB) Task Force on [57]

In February 2017, the Final Report of the U.S. Defense Science Board (DSB) Task Force on Cyber Deterrence was published.



The eight guiding principles for the DoD and U.S. Government are:-

- Deterrence by cost imposition requires understanding what key adversary decision makers value, holding that which they value

at risk, and communicating the credible will and capability to respond.

- Deterrence by cost imposition requires credible response options at varying levels of conflict.
- In the event of a cyber attack on the United States (i.e., a failure of cyber deterrence), the question should not be whether to impose costs in response, but how and when to do so against the attacker, and how to connect the response to the attack.
- The United States must clarify that it seeks to deter and will aim to impose countervailing costs in response to some forms of costly cyber intrusions.
- Responding to adversary cyber attacks and costly cyber intrusions carries a risk of escalation and intelligence loss, but not responding carries near-certainty of suffering otherwise deterrable attacks in the future.
- Reducing the vulnerability of US critical infrastructure is essential not only to deterrence by denial, it also reinforces the credibility of U.S. threats to impose costs on attackers.
- Cyber arms control is not viable, though norms and rules of the road may be both viable and highly valuable.

Three sets of initiatives to bolster deterrence against the most critical cyber threats and related challenges to the United States were recommended as follows:-

- Plan and Conduct Tailored Deterrence Campaigns. One size will not fit all adversaries from peacetime to "grey zone" conflicts to war.
- Create a Cyber Resilient 'Thin Line' of Key U.S. Strike Systems. It should boost the cyber resilience of select US strike systems like cyber, nuclear, non-nuclear and supporting critical infrastructure to

ensure that the U.S. can realistically threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attacks.

- Enhance Foundational Capabilities. US Government must pursue diverse capabilities, such as enhancing cyber attribution, the broad cyber resilience of the joint force and innovative technologies that can enhance the cyber security of the most vital U.S. critical infrastructure.

Planning for cyber deterrence operations will have the following challenges:-

- An adversary might conduct cyber attacks, in widely varying contexts from peace to grey zone conflict to the severe crisis to war.
- Campaign planning must be an integral part of a broader political-military campaign and other diplomatic and military actions.
- Effects of cyber attacks can be highly uncertain and attribution may be difficult in some cases.
- Planning must engage senior national security leaders to make complex judgments under tremendous ambiguity about a range of issues including adversary leadership views, the risks of escalation in varying contexts and the specific impacts of both adversary and U.S. cyber actions on the strategic interests of the United States.

The call for a comprehensive cyber deterrence strategy is summarized as, 'In the face of an escalating threat, the U.S. DoD must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non state actors from conducting cyberattacks against U.S. interests.' Because of the variety and number of state and non state cyber actors in cyberspace and the relative availability of destructive cyber tools, an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors' behaviour.

Example of the U.S. Cyberspace Solarium Commission (CSC) [58]

The U.S. Cyberspace Solarium Commission (CSC) was established to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The Cyberspace Solarium Commission published its final report on March 11, 2020. The 182-page document is the culmination of a year-long, bipartisan process to develop a new cyber strategy for the U.S. The Cyberspace Solarium Commission's suggests a strategy of layered cyber deterrence. The report consists of over 80 recommendations to implement the strategy. The Chairman, in his forward note, outlined the following big ideas:-

- Deterrence is possible in cyberspace.
- Deterrence relies on a resilient economy.
- Deterrence requires government reform.
- Deterrence will require private sector entities to step up and strengthen their security posture.
- Election security must become a priority.

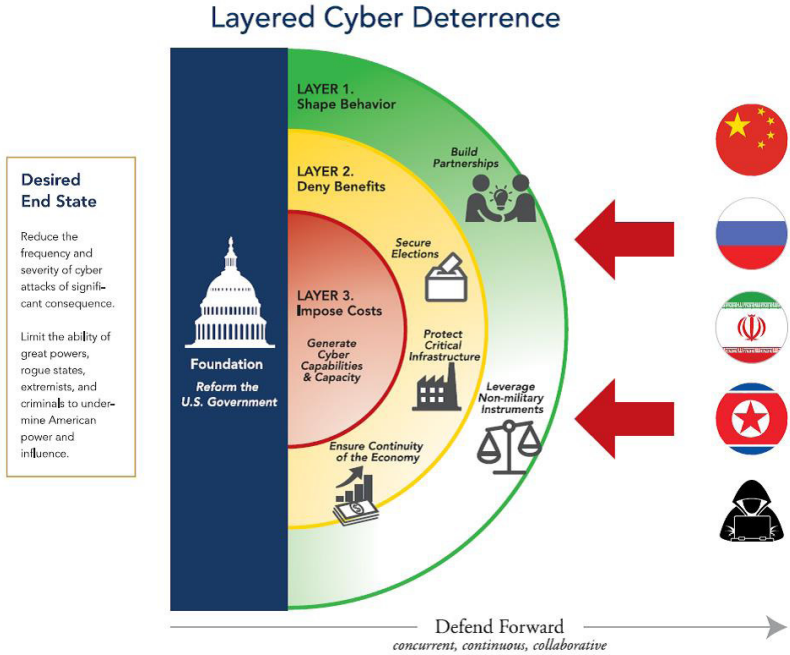
The Idea of Layered Cyber Deterrence

The Commission advocates a novel strategic approach to cyber security called 'layered cyber deterrence'. The desired end state of layered cyber deterrence is a reduced probability and impact of cyber attacks. The strategy outlines three ways to achieve this end state:-

- **Shape Behaviour**. Work with allies and partners to encourage responsible behaviour in cyberspace.
- **Deny Benefits**. Deny benefits to adversaries who have long exploited cyberspace to their advantage and at little cost to themselves. This new approach requires securing critical networks in collaboration

with the private sector to promote national resilience and increase the security of the cyber ecosystem.

- **Impose costs**. The U.S. must maintain the capability, capacity, and credibility needed to retaliate against actors who target America in and through cyberspace.



Source: Senator Angus King, Cyberspace Solarium Commission, 11 Mar 2020 available at: https://www.solarium.gov/

Concept of Defend Forward and Layered Cyber Deterrence

Layered cyber deterrence places a concept of defending forward in a broader, whole-of-nation framework that uses multiple instruments of power to secure own networks in cyberspace. The connectivity and global reach of cyberspace make forward defence essential today. Operationalising defend forward and persistent engagement requires three key actions:-

- Plan, resource and conduct cyber operations and standing campaigns to counter adversaries. This includes countering adversaries' offensive cyber capabilities and infrastructure, organisations that support their cyber operations and campaigns and the locus of their decision making.

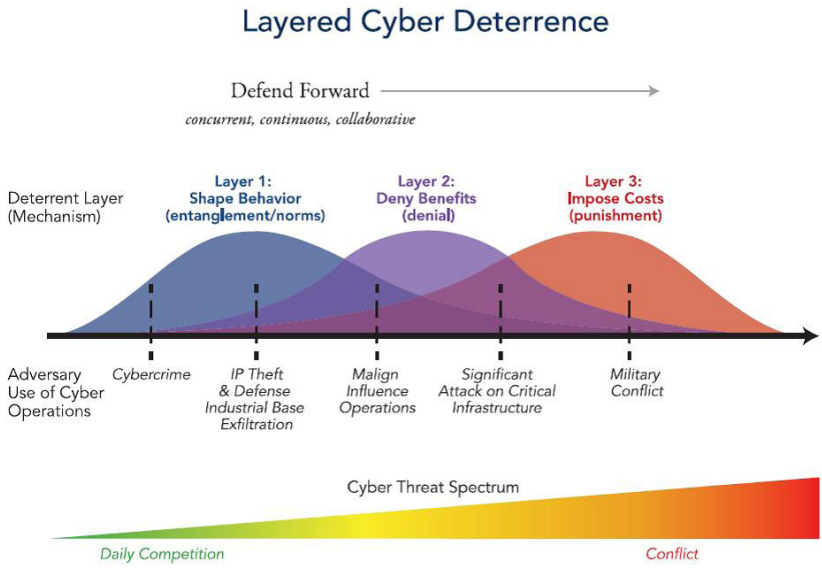
- Have capabilities and processes within the cyber force to rapidly respond to emerging geopolitical situations and ensure that these cyber capabilities can be easily integrated with other military and non-military tools. The military should develop the capacity to provide decision makers with cyber options, including choices to support crisis bargaining and response options.

- Operate in cyberspace to provide early warning, gain situational awareness of evolving adversary tactics, techniques, and procedures (TTPs), capabilities and personas. Conduct operational preparation of the environment. The cyber domain is dynamic, opportunities are fleeting and adversaries are agile and adaptive.

When these three elements are combined, the military component of defending forward can be integrated as part of a whole of government effort with other instruments of national power. These include diplomacy, information, the military, economic and financial tools, intelligence and law enforcement. Layered cyber deterrence will change the cost-benefit calculations of the adversary to threaten own interests in cyberspace. It is difficult to stop all cyber activities of state and non-state actors engaged in espionage, military operations, political warfare or criminal activity. The aim is to reduce the severity and frequency of cyber activity. Layered cyber deterrence depend on robust public-private collaboration to ensure that national cyber strategy does not remain confined to the defense sector.

The three layers deliver overlapping visions of networked cyber strategy to defend the nation as it meets new methods of digital warfare. The end state is to reduce the overall frequency and severity of cyber operations. The

first layer is an extension of entanglement strategies. It considers shaping the international environment critical for the development of cyber stability. It would enable allies to collaborate to create norms, regulations and institutions to encourage responsible action in cyberspace. The second layer incorporates some traditional aspects of deterrence, especially resiliency and defence in depth. This effort comprises protecting critical infrastructure, securing elections and ensuring the stability of the economy and government. The third layer imposes costs and seeks to generate cyber capabilities and capacity. This is a critical method of applying force to coerce in cyberspace. The restoration was required after it was eliminated in the concept of persistent engagement.



Source: Senator Angus King, Cyberspace Solarium Commission, 11 Mar 2020 available at: https://www.solarium.gov/

The strategy of layered cyber deterrence could become difficult if the layers culminate in working at cross purposes with each other. For example, one department's efforts to create standard norms can conflict with the defense department's offensive cyber initiatives.

Layered cyber deterrence aims to alter how states compete and deter attacks in the cyber domain above and below the threshold of armed conflict. This can be achieved by a stable expectation of norms, denying attack surfaces to the opposition, enabling resilience in defence, and making clear, credible commitments to impose costs.

Section 9: Critical Issues of Cyber Deterrence

Practical Limitations of Cyber Deterrence

The classical concept of strategic deterrence has its limitations in cyberspace. During Cold War, deterrence was symmetrical and applied by approximately likewise strong actors who were able to assess their motives thoroughly. Cyber deterrence is multipolar. It takes place between asymmetric opponents. The analogy of nuclear deterrence is misleading. Cyber capabilities are mostly opaque and can proliferate quickly. Risk of deterrence failure increases with problems of attribution, anonymity, advantage of attacks, global reach and interconnectedness, controllability and the credibility of digital capabilities and displays of power. Cyber operations are not always publicly acknowledged by either side. Cyber deterrence can fail quickly and is not a reliable policy option. One is not sure what kind of capabilities the adversary might have and how they are using them. Employment of non state actors to carry out offensives gives any state a higher degree of plausible deniability.

Deterrence is mainly about messaging or the ability to communicate boundaries and consequences. Martin Libicki renders the core message of deterrence as "if you do this then that will be done." The ability to send that message requires the following:-

- **Attribution**. The state should be able to define the target of

retaliation.

- **Thresholds**. The state should be able to distinguish consistently between acts that merit retaliation and those that do not.
- **Credibility**. The state's will to retaliate should be believed.
- **Capability**. The state should be able to pull off a successful response.

The focus on cyber-deterrence is reasonable but misplaced. Aim of the deterrence is to change the calculations of adversaries by encouraging them that the risks of an attack offset the rewards or that they will be denied the benefits they seek. Deterrence can be effective if one can build and demonstrate offensive cyber capabilities. Offensive cyber capabilities are an essential element for the nation-states to succeed in their current and future international and security policies.

Glaring weaknesses of U.S. deterrence policy got highlighted by two incidents: the 2014 hacking of Sony Pictures attributed to North Korea and the 2015 cyber attack on the U.S. Office of Personnel Management (OPM), attributed to China. The Sony episode revealed three notable shortcomings in U.S. cyber-deterrence policy:- [59]

- Persistent ambiguity about the government's role in responding to attacks on privately owned information infrastructure.
- Inability to coordinate a unified response by the government and private industry to the threats.
- Media was willing to report on the substance of the hacked e-mails brought to light by an aggressive foreign actor. It failed to highlight the motives behind the hacking.

The recent Ransomware attacks on U.S. critical infrastructure has exposed the limitations of deterrence capabilities of a powerful country like U.S. Although most individual ransomware attacks fall below the use of force as defined in international law, collectively the ransomware attacks threaten

national security, economic prosperity and public health and safety

Ron Bushar, senior vice president of Mandiant, speaking to Sea Air Space Conference August 2, 2021 said, "These attacks are rapidly outpacing our ability to innovate, defend against cyber tools and weapons and vulnerabilities that are the same problem. As we accelerate technology, innovation, and software development, we can't keep up with the human mistakes that get put into code everywhere we see it….. I don't think we've hit a real deterrence level in this space yet. And that's going to be key to thinking through our strategy over the next few years." He said that pursuing a primarily diplomatic strategy that "doesn't have any real deterrence mechanisms built into it beyond kind of naming and shaming" is unlikely to be effective in the long run. He said that the U.S. and its allies "have to think about attribution as a strategic imperative, not just as a nice-to-have. We have to get away from this model of, let's go higher with cyber walls, right? Let's deter our adversaries or prevent our adversaries from getting into our environments."[60]

Failure of Deterrence [61]

U.S. Example. The concept of deterrence hasn't held up in recent years. The ability to deter actors in cyberspace remains a source of contention in policy making and academic circles. The U.S. has faced dozens of state-backed cyber attacks from virtually every one of its adversaries. A number of recent high-profile cyber operations including the SolarWinds hack by Russian cybercriminals[62] and the Microsoft Exchange hack by China[63] created doubts about the capability of the U.S. to defend itself and advance its interests in cyberspace. In response, President Joe Biden, In May 2021, released a detailed executive order[64] **to improve the nation's** cyber security.

Russia. During the 2016 U.S. presidential campaign, Russian hackers broke into the Democratic National Committee's e-mail servers and made efforts to influence the election's outcome. Russia has carried out a series of attacks testing the defences surrounding critical U.S. infrastructure,

targeting the U.S. electricity grid and its operators. It made efforts to manipulate elections in 18 other countries. U.S. intelligence agencies and cyber security companies have connected Russian hackers to the shutdown of a German steel mill, the cutting off of phone and Internet service to some 900,000 Germans, and two disruptions of the power grid in Ukraine. This should be a warning about what damage can be done in the cyberspace.

China. Chinese hacking groups have stolen U.S. intellectual property from industrial manufacturers and military contractors. In 2015, China weaponised its 'Great Firewall' and conducted distributed denial of service attacks against U.S. websites e.g., against GitHub, which Beijing wished to punish for hosting content that the Chinese leadership found undesirable. Chinese cyber attacks against U.S. infrastructure and network probes continue to be a key U.S. concern.

North Korea. In 2014, North Korean hackers attacked the U.S. film studio Sony Pictures to block the release of a movie. The attack erased the content of thousands of computers, released embarrassing internal e-mails and intimidated Sony into cancelling the movie's theatrical release.

Iran. Iran has carried out attacks against U.S. financial institutions and a dam in New York.

Both Russia and China have shown a repeated willingness to criminalise the cyberspace. Short of preventing a significant loss of life or economic activity, Chinese and Russian actions show that the U.S. doctrine of deterrence has failed at the lower and middle levels. North Korea and Iran have pursued targeting actions in the cyberspace despite the threat of retaliation. The situation has led to fresh calls for cyber-deterrence measures that would impose higher costs on would-be hackers while denying them the benefits.[65] The Trump administration has elevated U.S. Cyber Command to a unified combatant command, which it believes will signal greater capability and resolve.[66]

Building deterrence is not merely about military capability. There has to be a unified strategy that cuts across agencies. It should be willing to understand and use all the tools of power and policy and not only those that encompass the zeroes and ones of software or malware.

Theoretical Limits of Deterrence in Cyberspace

Differences between the kinetic and cyber operations pose serious problems when deterrence theory is applied in cyberspace. While the problems of attribution and proportionality are known, there is no agreement on how they can be solved. Some advocate that these problems are unsolvable and deterrence will eventually be ineffective in this domain. Lan and colleagues stress that "the anonymity, the global reach, the scattered nature, and the interconnectedness of information networks greatly reduce the efficacy of cyber deterrence and can even render it completely useless.[67]

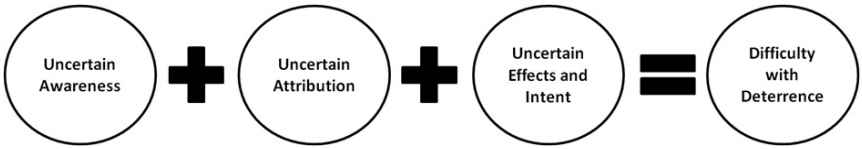
There is also an opposite view which feels that deterrence could play a crucial role in averting cyber conflicts and their escalation. Whether deterrence theory offers the right framework for cyber deterrence or a new theory of deterrence is the question. Deterring potential aggressors depends greatly on the perceived (that is, in the minds of the aggressor) ability of a defender to survive and attribute attacks and the defender's readiness and ability to respond to attacks.

Deterrence by threat in cyberspace is realistically applicable to cyber operations that result in direct physical effects that are non-repudiable and attributed quickly. The anonymity connected with attacks is necessary for attacks to be successful in bypassing deterrence by denial frameworks found in the perimeter defences of the logical or physical network layers. There are some fundamental challenges exclusive to cyberspace posed by anonymity.

Peter Singer of the Brookings Institution and others have identified this lack of attribution as the main factor that prohibits the direct and immediate application of deterrence theory to the cyber realm. If an

attack is attributable, then traditional deterrence is applicable, including the likelihood of a kinetic response. If it is not attributable, or the attacker believes it will be falsely attributed, it may be so enticing a weapon as to be irresistible.

Challenges in applying Deterrence Theory to Cyber Warfare



The kind of retaliations or other forms of punishment and non-viable solutions for most retaliations in cyberspace are:- [68]

- The state is responsible to produce the proof in identifying the perpetrator of an attack. The potential for retaliation depends upon attribution of who, what, and why an attack occurred. Absence of solid evidence is likely to lead to mis-identification and unnecessary escalation.

- The state must retaliate within a close temporal range. If a state does possess detailed intelligence on the target it wants to retaliate against. Developing intelligence along with a cyber weapon to target it increases the time period of response. It may take anything from days to years. Due to this temporal disconnect, the threat to punish a given action in response falls into a category of hyperbolic discounting. It can be discounted to the point of irrelevance.

- Deterrence by punishment needs proportionality. It is essential to have comparable assets to punish to prevent escalation or violations of international law. Comparable assets are often difficult to identify. To punish an asset needs pre-established access or knowledge of that asset. A computer or a network system that is penetrated today

for prepositioned access, might be patched, upgraded or taken offline tomorrow.

- A state must have a specific cyber weapon system tailored to its target. An old or repeated weapon is likely to be ineffective as the defender might have updated perimeter defences using defence in-depth by anti-virus programs, firewall intrusion detection and prevention systems (IDPS) or a variety of other security measures.

Though deterrence by punishment in cyberspace is possible, it is not a reliable or credible option. This assessment is not unique. Analysis by Valeriano and Maness, shows that deterrence via punishment is generally ineffective and likely more dangerous than other means of preventing attacks.[69] Furthermore, sustained invasive intelligence into adversary networks creates its own unique problems, including a security dilemma.[70]

Allocation of resources between deterrence and denial and the effectiveness with which they deter adversaries vary. Setting up of credible deterrence by denial often starts with allotment of funds to buy technical resources and make available human capital sufficient to continually update, enhance, audit and manage complex network infrastructure.[71]

Section 10: Chinese Concept of Cyber Deterrence

PLA's Definitions

The Science of Military Strategy of China defines deterrence as "the strategic operation, with the threat to use or the actual use of military capability in order to influence the adversary's strategic judgments by making the adversary feel it is difficult to achieve anticipated targets or

the cost may exceed the benefit, conducted by countries or political groups for certain political goals."[72] Chinese official publications emphasise the importance of linking deterrence actions to political objectives. The PLA dictionary of military terminology of 2011 defines a strategy of deterrence as a military strategy of displaying or threatening the use of armed power to compel an opponent to submit. It categorised deterrence into offensive, defensive deterrence, conventional, nuclear, comprehensive or limited deterrence. A classified manual for the PLA's Second Artillery, now the PLA Rocket Force, published in 2004, defines the purpose of campaign deterrence as to compel an enemy to accept own will or to contain an enemy's hostile actions. It states, deterrence is a tool for achieving policy objectives, and it is intended to support China's overall national strategy.

Strategic Deterrence

China feels, "Strategic deterrence is a major means for attaining the objective of military strategy, and its risks and costs are less than strategic operations…. Strategic deterrence is also a means for attaining the political objective." Deterrence "may fail and even war or war escalation may be triggered if one mishandles the complex situation." Therefore, "war fighting is generally used only when deterrence fails and there is no alternative, and the more powerful the warfighting capability, the more effective the deterrence." There is a complete Section on Strategic Deterrence in the 2005 edition of The Science of Military Strategy.

Strategic deterrence includes nuclear deterrence. Besides, it comprises of information, space and cyber operations. It also contains the 'deterrence of people's war;, and involves other government agencies and civilian capabilities.[73]

The Science of Military Strategy published in the 2013 edition also has a Section on deterrence. It highlights the basic principles from the earlier version and updated them according to changes in the international security environment and technological advances, especially in the PLA's

level of information technologies, space, and cyber capabilities.[74]

Deterrence in Cyberspace

Some Chinese scholars feel that applying deterrence to cyberspace is different from conventional deterrence. They think that attribution is difficult, detection and monitoring are yet to mature and that the effectiveness of a cyber attack is uncertain.[75] The Science of Military Strategy concluded that there is "very great diversity in different people's understandings of network deterrence and the theory and practice of network deterrence both await further development and perfection."[76] A noted scholar on China, Dean Cheng, notes that Chinese defence analysts traditionally view deterrence, or weishe, threats intended to raise the costs high enough, so a potential adversary does not act in the first place; and as compellence, displays of military power or threats to use military power to compel an opponent to take action or submit.[77]

A researcher at the Academy of Military Sciences, Yuan Yi, describes deterrence by "combat operations when one side believes the other is on the verge of initiating war, it may launch cyber attacks on critical defensive networks, thus conducting 'preventive, restraining deterrence'. As per Yuan Yi, a successful deterrence strategy requires preparation. Cyber forces must conduct comprehensive network reconnaissance and install backdoors and logic bombs to launch future attacks. The Chinese writers on offensive cyber operations emphasise the necessity "to remind an adversary of one's ability to plant viruses or otherwise undertake information attacks to warn them to cease their policies or otherwise coerce them."[78] Yuan Yi summed up the strengths of cyber deterrence due to:-

- Cyber attacks are more humane than nuclear, biological or chemical attacks.
- Deterrence is cost-effective as cyber weapons are cheap.

- Deterrence methods are diverse since cyber weapons can target multiple types of systems.
- Deterrence uses are repeatable and flexible as, unlike nukes, cyber weapons can be used multiple times.

Weaknesses of Cyber deterrence are stated as follows:-

- Lacks credibility because cyber weapons have not yet been used in real warfare.
- Cyber defence is dynamic and may eliminate vulnerabilities making a weapon useless.
- Effects of a weapon may spread to connected networks and may even boomerang back to the attackers.
- States with low levels of connectivity provide few targets and are not easily deterred.
- Distributed nature of networks makes the creation of a unified military force difficult.

Yuan Yi outlines four types of deterrence. Three are by appearance and the fourth by actual combat.

Deterrence by Appearance. It includes technical tests with widespread publicity about the results as well as the displays of cyber equipment. Displays can happen through doctrine, white papers, diplomatic pronouncements, media or other official channels. It can happen through social media and may involve misinformation to confuse the enemy and create a psychology of fear and restraint. Combat exercises are a method of deterrence by appearance. It may involve real or virtual troops. 'Cyber Storm', the biennial exercise run by the U.S. Department of Homeland Security is an example of deterrence by exercise.

Deterrence by Combat Operations. Here, the Opportunities are stated to be as follows:-

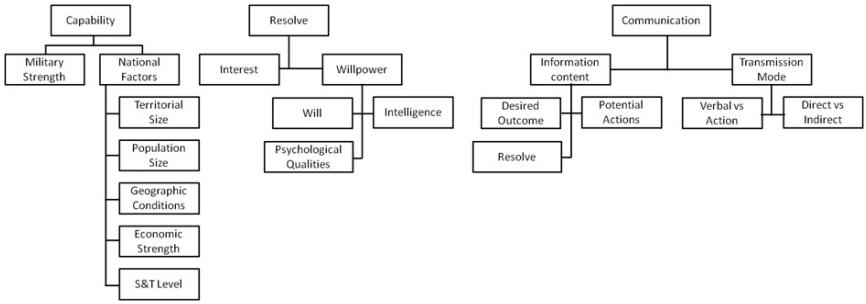
- When one side considers that the other is about to start a war, it may launch cyber attacks on critical defensive networks, thus conducting "preventive, restraining deterrence."
- When the enemy is conducting cyber attacks, you must immediately launch "retaliatory, reprimanding deterrence." The types of attacks could be disseminating propaganda on cell phones and interrupting television broadcasts and damaging telecommunication networks and power grids.

A successful deterrence strategy requires preparation. China believes that cyber forces must carry out extensive network reconnaissance and install malware, backdoors and logic bombs to facilitate future attacks. Decision-makers need to find the right balance to achieve combat deterrence. Restrained attacks will not dismay the enemy. Extensive damage may incite a conventional military response. There should be a controlled escalation ladder. A strong deterrence strategy demands centralised command and unified planning. The decision-makers "must organize and coordinate amateur civilian cyberwar forces, particularly patriotic hackers."[79]

China's definition of deterrence encompasses more than the traditional definition. It includes compellence. Some Chinese scholars have stated that China's thinking about deterrence roughly approximates Schelling's broader concept of coercion.[80]

The Chinese concept of deterrence remained consistent over time. However, it has evolved with some significant exceptions, e.g. rising importance to the space and cyber domains and a launch on warning posture for China's nuclear missile force.[81]

Core Components of Chinese Deterrence

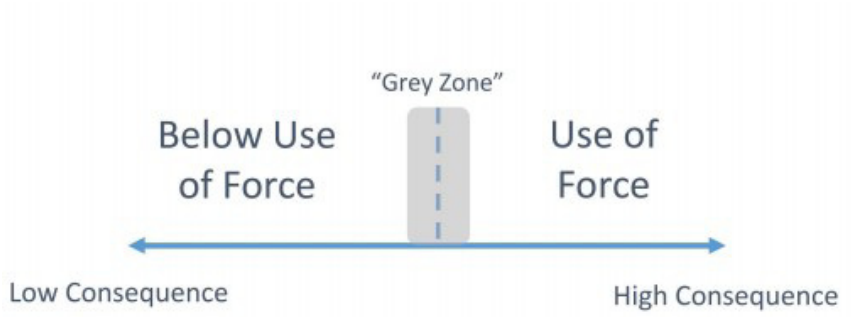


SOURCE: Academy of Military Science Military Strategy Department ed., Science of Military Strategy, 3rd ed., Beijing: Academy of Military Science Press, 2013, pp. 135–137.

Section 11: Cyber Deterrence Policy – The Way Ahead

Certain activities like espionage cannot be deterred realistically. Destructive cyber attacks against critical infrastructure assets by nation-states outside of armed conflict can possibly be undertaken. Between these two types, a range of malicious cyber activities take place. Some state, non-state actors and cyber criminals exploit this gap. They use their cyber capabilities to cause harm, but below a threshold level which do not ask for retaliation by cyber or kinetic means. Recent Ransomware attacks are good examples.

Currently, malicious cyber activity in this grey zone is causing long-term damage to national security, economic prosperity and public health and safety in both the digital and physical worlds. The like-minded nations should try to implement a set of cyber deterrence policies that would reduce the size of the deterrence gap of the grey zone, reduce the intensity, volume and impact of malicious cyber activity that is carried out within this zone and strengthen agreed upon norms of behaviour in cyberspace.



Source : Eva Uribe and Michael Minner, Cyber Deterrence and Resilience Strategic Initiative: Intern Briefing available at: https://www.osti.gov/servlets/purl/1806268

However, there are some misconceptions. Cyberspace is not borderless. Every router, firewall, switch, and network equipment creates a boundary. Cyber borders do not align with the physical borders and boundaries. Cyber borders follow their own rules and logic, which are different from nation-state political structures. However, cyberspace is not entirely divorced from the physical world. All the computers, servers, network equipment like routers, switches, servers, and Internet-of-Things devices exist somewhere in this world, always in some country's territory. Though the geography of cyberspace varies from that of the physical world, it is not entirely separate either.

In cyber deterrence models, factors like technical capability, private sector, non-state actors, non-profit organisations like non-government organisations (NGO) and some individual citizens are required to be included. Today non-state actors dominate the cyberspace ecosystem. The Internet is run through a multi-stakeholder model. Cyber deterrence policies must include the private sector, telecommunication companies, cyber security and cloud service providers, NGOs, international organisations, civil society, and critical infrastructure owners and operators rather than only the national governments.

Cyber security vendors can pass their technical understanding of how networks and devices function and their intelligence to help identify

targets. Internet Service Providers, Cloud Service Providers, and Hosting Providers can emphasise on disrupting the adversary's technical infrastructure. Civil society and NGOs can bring together the disparate players and ensure a broader picture of what is occurring. Governments should focus on taking direct action against malicious actors. A more comprehensive approach to cyber deterrence would have a multiplier effect by leveraging different organisations' comparative advantages. For governments, a significant challenge is engaging the non-state actors in a way that does not treat them as subordinates but as partners.

The level of organisation and coordination required for effective cyber deterrence policies is much higher than in traditional deterrence efforts. It requires more time, effort, patience and energy. As the government cannot compel anybody to collaborate, non-state actors' willing participation becomes essential. The overlapping and sometimes ambiguous nature of the targets of deterrence makes it complex and challenging. In cyberspace, the line between nation-state, non-state actors and criminals has become fuzzy. Russia uses criminal groups as proxies. North Korea is carrying out criminal activities to circumvent international economic sanctions. Nation-states and cyber criminals carry out malicious cyber activity for essentially different reasons.

Cyber deterrence policy has to address these different motivations concurrently. Cybercriminals spend limited time and resources to access any given target's network. If it is too difficult or time-consuming, they shift their attention to other likely victims. Here deterrence by denial can prove highly effective against cybercriminals. On the other hand, to advance its national-security goals, a nation-state can spend much more time and resources to access that target. Cyber deterrence policy must combine military and criminal deterrence components to deter different motivations and specific situations. Diplomatic, law enforcement, technical counter-cyber operations and economic penalties should also form part of that array.

The private sector has a significant role to play to build resilience. Internet service providers, critical infrastructure providers, operators of social media platforms, the military and the government, have vital roles in ensuring service continuity in the event of major cyber disruptions. Internet Service Providers and internet content creators may be able to deter cyber attacks by self -policing and making their networks resilient to malicious use. Commercial players must make their products safe, secure and free from attack and manipulation. Measures have to be put in place to keep the internet running, minimise the impact of cyber attacks and quickly replace core services.

Such a strategy will rely on effective communication and efficient information sharing between government and the private sector. The resilience strategy should not be viewed as replacements for other cyber deterrence approaches. Tim Ridout has argued for combining resilience with other forms of cyber deterrence, "resilience could play a critical dissuasive role by reducing the utility of cyber offence, especially when joined with the credible threat of punishment. If you demonstrate that you can absorb a blow, bounce back quickly, and then hit back, resilience and deterrence can be a potent combination." Expanded cyber deterrence policies should differ in five ways: clearly defining the new activity to be deterred, using comparative advantage, explicitly linking cyber issues with non-cyber issues, encompassing more than technical cyber actions and involving active disruption.

All is not lost. Even cyber criminals try to maintain a degree of anonymity and avoid travelling to Western nations to avoid being caught. Some minimal level of deterrence operates even against cybercrime. Luckily, most organisations are convinced of the need for concerted international and multi-stakeholder models to uphold norms of good behaviour in cyberspace. They are waiting for a suitable engagement forum to materialise. The recently concluded first round of the United Nations First Open-Ended Working Group (OEWG) on Information Communication

Technology (ICT) challenges in the context of international security showed how important it is to reach out to non-state actors.[82]

Deterrence of cyber attack has failed in the past and will fail in the future. Policy must worry about re-establishing deterrence when it fails and the related concept of cumulative deterrence. Deterrence may or may not be the most credible or effective strategy for achieving desired end states in cyber security. It will require a complex mixture of resilient, well-defended cyber infrastructures, careful use of offensive cyber operations, and deterrence strategies to dissuade adversaries from taking undesirable actions.

Deterrence is always a key component of any cyber strategy. However, there is very little detail available on how to operationalise or implement this policy, how to bring a whole-of-government and whole-of-private sector approach to cyber deterrence, which types of opponents can or should be deterred, and in which contexts. Nation states are using cyber operations below the threshold of armed conflict to produce effects or to generate coercive options for themselves if conflict escalates above this threshold. The 2018 Command Vision of the U.S. Cyber Command recognises that "adversaries operate continuously below the threshold of armed conflict to weaken our institutions and gain strategic advantages."

Deterrence Requirements for Various Types of Deterrence Strategies is given at Appendix A.

Non-state Actors

Differences in deterring a non-state actor and a nation-state. The following differences between non-state actors and nation-states make deterrence of violent non-state actors a far more complex and challenging task.

- Unlike states, non-state actors do not exercise sovereignty over a given territory. They often want to weaken the state's credibility by attacking its ability to exercise sovereign control over its territory.

Non-state actors can deter states successfully than states can deter their non-state adversaries.

- Non-state actors do not have clearly identifiable centres of gravity that can be easily targeted. For a nation-state, the capital, political leadership or military forces usually function as the centres of gravity.

- Unlike nation-states, non-state actors exist to change the status quo. States have an inherent desire to protect, which they already possess. It makes them susceptible to coercion if they desire a change in the status quo.

Few states, if at all, have national deterrence strategies aimed at non-state actors, criminal organisations or individuals. The view from most scholars and practitioners are likely to be that it is not the responsibility of the state to deter non-state actors (excepting terrorists) and criminals from waging cyber attacks against non-federal infrastructure. Nevertheless, the same tools used by a criminal are available to the state and present the same challenges related to attribution irrespective of the perpetrator. The incidence of Russian influence and hacking during the 2016 election cycle in the U.S. is an example of why deterrence by threat in cyberspace is so difficult to achieve. The FBI identified the first indications of Russian interference in the 2016 election in September 2015, more than a year before the election.

Paradoxically, deterring states from acts of force is easier than deterring non-state actors from actions that do not rise to the threshold level of force. Major state actors are entangled in interdependent relationships. There are many non-state actors. The U.S. policy has made it clear that deterrence is not limited to cyber against cyber only but can be cross-domain, including naming and shaming, economic sanctions and nuclear weapons. Non-state actors are more in number and often difficult to identify. The SolarWinds

and Microsoft Exchange hacks avoided sophisticated Sometimes they act as proxies for states. The self-proclaimed Romanian blogger 'Guccifer 2.0' is a front for Russian intelligence in the release of the Democratic National Committee emails in 2016. NSA detection capabilities by launching their tools from inside the U.S., where NSA does not operate. U.S. intelligence agencies did not even detect the 2020 SolarWinds and Microsoft Exchange attacks for as long as nine months (SolarWinds). Official attribution of SolarWinds was not announced until April 2021. This creates problems for deterrence in the cyber realm.

Punishment is possible against non-state actors and criminals, but the slow attribution process blunts its deterrent effects. Denial plays a significant role in dealing with non-state actors. With time and effort, a major military or intelligence agency is capable of penetrating most defences. Cost-benefit analysis is vital in these cases.

Role of Third Parties

Some forms of 'patriotic hacking', where individuals or groups carry out website defacement, compromise of personal data and distributed denial-of-service attacks are nowadays invariably done in any conflict. Third parties engaged in cyber attacks complicate signalling and escalation control. Martin Libicki argues that "exchange of cyber attacks between states may also excite the general interest of superpatriot hackers or those who like a dog pile—particularly if the victim of the attack or the victim of retaliation, or both, are unpopular in certain circles." For example, during the war in Gaza in 2012, the hacktivist collective group 'Anonymous' launched its '#OpIsrael Campaign', attacking websites belonging to the Israeli Defense Forces, the prime minister's office, Israeli banks and airlines. Non-state actors create problems for deterrence in the cyber domain as they are much more in number than states and often difficult to identify. Sometimes they are proxies for states.

Deterrence is less effective if the adversary is a non-state actor or does

not have much value to hold at risk for retaliation, or it is not rational. Even for a strong state, intrusions into critical networks will still cause concern. Tough cyber hygiene and defences may reroute some non-state actors to other acts and means. Criminals and terrorists may be deterred by denial, such as shifting work factors that cost them time and resources and disrupt their business models.

Occasionally non-state actors can add to deterrence. States can benefit from the deterrent actions of non-state actors. These include the attribution efforts of private security companies concerning punishment, international and transnational organisations' entrepreneurial activities in norm creation and enforcement, or multinational companies' actions in entanglement. Sometimes non-state cyber vigilantes take down websites and counter the online activities of criminals and terrorists.

Not everything that we might call a cyber attack is actionable. In the grey zone, deterrence works very differently if your adversary is sure they are striking back. Cyber operations may be the most escalatory kind of conflict one has seen. Any exercise in cyber deterrence must be thought of as an experiment. Some of the experiments will work, some won't. We have to be cautious, attentive to the evidence and willing to learn.

Conclusion

At least in the near future, for any country to launch pre-emptive or retaliatory cyber strikes against different threat actors will be difficult due to problems of attribution, ability to respond quickly, effectively and accurately and build and sustain a model by which repeatability can be leveraged. Cyber deterrence by denial has a better chance of success. But success would be limited as cyber network defence have been beaten consistently breached by agile, intelligent, tech-savvy adversaries obfuscating themselves in cyberspace. Nation-states should evaluate their current security postures and find out their effectiveness in the current cyber environment.

On the issue of 'Can Cyber Deterrence Work?' Martin Libicki states, "The goal of cyber deterrence is to reduce the risk of cyber attacks to an acceptable level at an acceptable cost," where the defending nation-state mitigates potential offensive action by threatening a potent retaliation. Though cyber deterrence operation may not be executed in a vacuum, it is not clear whether such a policy is successful. Taking offensive cyber operations for defensive purposes does not nullify the requirement of an overall, in-depth cyber defence posture. Traditional cyber defences will be very much required. A cyber expert from the Center of Strategic & International Studies, Jim Lewis, states that "survey data consistently shows that 80-90 per cent of successful breaches of corporate networks required only the most basic techniques, and that 96 per cent of those could have been avoided if proper security controls were in place." The most basic computer security practices would still be required to achieve maximum cyber security coverage.

Deterrence by Punishment counts on the rationality of actors. It will only work if the people/groups/government being deterred are rational. They can be deterred due to their unwillingness to risk losing something of greater value. Presently, adversaries operate in cyberspace without fear of retaliation because attribution challenges and the unsecure environment favours their actions. A nation-state is more conducive to deterrence than a terrorist or hacktivist organisation. The adversary must have something of value which can be targeted for a pre-emptive/retaliatory strike to be effective. If he doesn't have that kind of target, the threat of cyber deterrence becomes irrelevant.

Effective cyber deterrence policies require regular, sustained disruption of malicious cyber activity. Such disruption can be technical, legal, logistical, financial, diplomatic, and, in some extreme cases, kinetic. Increasing the scope, scale and tempo of disruption activities should impose high costs on adversaries. Deterrence is not credible unless it is backed by clear, decisive action. Integrating non-cyber tools like economic sanctions,

diplomacy, financial system constraints, law enforcement action, civil legal processes and even military action is required for effective cyber deterrence. Technical cyber actions will form a small but important part of it. Cyber deterrence policies will have a wide range of tools in their arsenal. The tools that will have the most significant effect on the intended target would be selected. Cyber criminals are primarily interested in money and use cryptocurrency for their payments. A very effective tool against them would be to bring the cryptocurrency exchanges to comply with global financial rules. Similarly, a nation-state actor may be more worried about diplomatic losses.

There is no proof till now that technical and organisational capabilities make the adversaries back down. On the contrary, there is growing evidence that they accomplish the opposite. Perhaps one cannot prove that deterrence is working. Nevertheless, one can definitely see if it isn't. Cyber conflict is a relatively new phenomenon, and its dynamics are still evolving.

Any act of cyber deterrence can be thought of as an experiment. Some will work, some will not. The best way is to think, act and then watch and learn. Cyber Deterrence uses force or threats of force to warn an adversary about the consequences of taking or failing to take any action.

Appendix A

Deterrence Requirements for Various Types of Deterrence Strategies

	Communicated	Credible		Capable		Calculated
		Rational	Principled	Executable	Painful/Costly	
Resistance	Norms: "XYZ values are an inherent part of who you are. Taking this action violates your core identity." Self-deterrence	The antagonist* perceives that holding these norms and being aligned with a like-minded COA is in their own best interests. (COA = community of actors)	The antagonist believes that these norms are fundamental to their identity and values.	The antagonist believes that taking the proscribed action incontrovertibly and undeniably violates the norms they hold dear.	The antagonist believes that taking the proscribed action is not worth losing their inherent sense of self.	The antagonist perceives that the protagonist believes that the antagonist is a rational actor, and that given enough information about the antagonist's interests, thresholds, and red lines, the protagonist can influence the antagonist's decisions.
	Persistent engagement: "The protagonist** has ramped up an effort to engage with the antagonist before they reach the protagonist's network, to generate tactical friction and force the antagonist to focus on defense instead of offense."	The antagonist perceives that the protagonist believes that persistent engagement is in the protagonist's best interests, that it is not too expensive and that it will not provoke	The antagonist perceives that the protagonist believes persistent engagement with cyber adversaries is aligned with the protagonist's values and principles.	The antagonist perceives that the protagonist is able to engage with the antagonist persistently (technical capability)	The antagonist perceives that persistent engagement by the protagonist within or around the antagonists networks will raise the antagonist's operational costs	

	Communicated	Credible		Capable		Calculated
		Rational	Principled	Executable	Painful/Costly	
		escalation or retaliation.			to unacceptable levels	
	Defense: "The protagonist has implemented sufficient measures to diminish the likelihood that the antagonist's attack will achieve the desired effect."	The antagonist perceives that the protagonist believes resistance measures are in its own best interests to create and implement (e.g. not too expensive).	The antagonist perceives that the protagonist believes resistance measures are in line with the protagonist's principles (e.g. do not violate certain rights or freedoms of citizens).	The antagonist has sufficient visibility into the protagonist's security to believe their attack would be ineffective. The antagonist believes that the protagonist's resistance measures are as consistent and effective as the protagonist claims.	The antagonist believes it would require too many resources to overcome the protagonist's resistance measures.	
Retribution	Punishment: Oven threat or precedent: "If the antagonist does X, the protagonist will respond with Y, which will =pose unacceptable costs on	The antagonist perceives that the protagonist believes it is in its own best interests to carry out punishment.	The antagonist perceives that the protagonist believes the retributive action is consistent with the protagonist's principles.	The antagonist believes that the protagonist can carry out the retributive action.	The antagonist believes the impacts of punishment would be unacceptably painful.	

	Communicated	Credible		Capable		Calculated
		Rational	Principled	Executable	Painful/Costly	
	the antagonist."					
	Entanglement: "The economies/ infrastructure/allies/etc. of the antagonist and protagonist are interdependent. Therefore, any action the antagonist takes against the protagonist may also impact the antagonist."	The antagonist believes that they are interdependent with the protagonist. The antagonist believes that the protagonist would allow/tolerate these interdependencies based on the protagonist's own best interests, or that they are unavoidable.	The antagonist believes that the protagonist would allow/tolerate these interdependencies based on the protagonist's principles or values, or that they are unavoidable.	The antagonist perceives that they are in fact interdependent with the protagonist in the way the protagonist claims.	The antagonist believes blowback/shared impacts of attack would be =acceptable.	
	Norms: "The global standard is XYZ. Violating this norm has unacceptable consequences."	The antagonist perceives that the protagonist or COA believe that the norm is	The antagonist perceives that the protagonist or COA believe that norm is	If attributed, the protagonist or COA can impose reputation costs on the	Reputation damage will result in unacceptable financial, social, or political costs for	

	Communicated	Credible		Capable		Calculated
		Rational	Principled	Executable	Painful/Costly	
	(COA = community of actors)	important to uphold for their own benefit/livelihood.	consistent with their values and principles.	antagonist.	the antagonist.	
Resilience	"The protagonist has previously demonstrated that the effects of the antagonist's attacks have been mitigated, or that they (the protagonist) have been able to recover promptly."	The antagonist perceives that the protagonist believes resilience measures are in its own best interests to create and implement (e.g. not too expensive).	The antagonist perceives that the protagonist believes resilience measures are consistent with the protagonist's principles (e.g. do not violate certain rights or freedoms of citizens).	The antagonist has sufficient visibility into the protagonist's resilience to believe their attack would be ineffective. The antagonist believes that the protagonist's resilience measures are as consistent and effective as the protagonist claims.	The antagonist believes it would require too many resources to overcome the protagonist's resilience measures.	

Source: Ann E. Hammer et al., Resilient Energy Systems and Cyber Deterrence and Resilience Strategic Initiatives, Sandia National Laboratories, September 2020 available at: https://www.osti.gov/servlets/purl/1668133

Endnotes

1. Bernard Brodie, The Absolute Weapon: Atomic Power and World Order (New York: Harcourt Press, 1946); and Strategy in the Missile Age (Princeton: Princeton University Press, 1959); Herman Kahn, Thinking about the Unthinkable (New York: Avon Books, 1962); and Thomas Schelling, Arms and Influence (New Haven, CT: Yale University Press, 1966).

2. Michael J. Mazaar, Understanding Deterrence, Santa Monica, Calif.: RAND Corporation, PE-295, 2018, p. 4. Michael S. Gerson, "Conventional Deterrence in the Second Nuclear Age," Parameters, Autumn 2009, pp. 32–48; John Stone, "Conventional Deterrence and the Challenge of Credibility," Contemporary Security Policy, Vol. 33, No. 1, 2012, pp. 108–123; Edward Rhodes, "Conventional Deterrence," Comparative Strategy, Vol. 19, No. 3, 2000, pp. 221– 253; Richard J. Harknett, "The Logic of Conventional Deterrence and the End of the Cold War," Security Studies, Vol. 4, No. 1, Autumn 1994, pp. 86–114.

3. Samantha Ravich, and Annie Fixler. Framework and Terminology for Understanding Cyber-Enabled Economic Warfare. Foundation for Defense of Democracies. February 23, 2017.

4. Karl P. Mueller, Conventional Deterrence Redux: Avoiding Great Power Conflict in the 21st Century, Strategic Studies Quarterly 12, no. 4 (Winter 2018): 78–79 available at: https://www.jstor.org/stable/26533616.

5. Richard K. Betts , The Lost Logic of Deterrence What the Strategy That Won the Cold War Can -- and Can't -- Do Now, Foreign Affairs, March/April 2013.

6. Mearsheimer, John J., Conventional Deterrence. Ithaca: Cornell University Press, 1990, p 23.

7. Lawrence Freedman, Deterrence (Cambridge, UK: Polity, 2004), p 26.

8. Robert J. Art, "To What Ends Military Power?" International Security 4, no. 4 (Spring 1980), p 6.

9. Joseph S. Nye, Jr., Deterrence and Dissuasion in Cyberspace, International Security 41, no. 3 (January 2017), p 45.

10. Thomas C. Schelling, The Strategy of Conflict, Cambridge, Mass.: Harvard University Press, 1960, p. 6 available at: https://www.hup.harvard.edu/catalog.php?isbn=9780674840317

11. Thomas C. Schelling, Arms and Influence, New Haven, Conn.: Yale University Press, 1966, p. 71 available at: https://yalebooks.yale.edu/book/9780300143379/arms-and-influence

12. Thomas C. Schelling, Arms and Influence (New Haven, CT: Yale University Press, 2008, reprint of the original 1966 edition). Thomas Schelling (1921–2016) taught in the economics department at Yale at the beginning of his career, and then moved

to the economics department at Harvard. He also served in the government and worked for the RAND Corporation. He ended his career at the University of Maryland. In 2005, he won the Nobel Prize in Economics. See, William Grimes, "Thomas Schelling, Master Theorist of Nuclear Strategy, Dies at 95," New York Times, December 13, 2016 available at: https://www.nytimes.com/2016/12/13/business/economy/thomas-schelling-dead-nobel-laureate.html

13. Adapted from Will Goodman, Cyber Deterrence: Tougher in Theory than in Practice, Strategic Studies Quarterly 4, no. 3 (Fall 2010): 102–35 available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a528033.pdf

14. Dr. James C. Mulvenon and Dr. Gregory J. Rattray, Addressing Cyber Instability: Executive Summary, The Atlantic Council, July 8, 2004 available at: http://www.acus.org/files/CCSA_Addressing_Cyber_Instability.pdf

15. Iasiello, Emilio, Cyber Attack: A Dull Tool to Shape Foreign Policy (Tallinn: NATO CCD COE Publications, May 2013), p 398.

16. Joseph Nye, Deterrence and Dissuasion in Cyberspace, International Security (Win- ter 2016/17), available at: www.belfercenter.org/publication/deterrence-and-dissuasion-cyberspace.

17. Richard A. Clark and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It, New York: HarperCollins, 2010, p. 189 available at: https://georgetownsecuritystudiesreview.org/2013/12/10/richard-a-clarke-and-robert-k-knakes-cyber-war-the-next-threat-to-national-security-and-what-to-do-about-it-harper-collins-2010/

18. William J. Lynn III, Defending a New Domain: The Pentagon's Cyberstrategy, Foreign Affairs 89, no. 5 (September/October 2010), p. 97–108.

19. Jonathan Solomon, Cybercdeterrence between Nation States: Plausible Strategy or Pipe Dream? Strategic Studies Quarterly (Spring 2011): p2.

20. James Igoe Walsh, Do States Play Signaling Games? Cooperation and Conflict: Journal of the Nordic International Studies Association 42:4 (2007): p 441.

21. Rid and Buchanan, Attributing Cyber Attacks, The Journal of Strategic Studies, p. 31 available at: https://ridt.co/d/rid-buchanan-attributing-cyber-attacks.pdf

22. Iasiello, Emilio, Is Cyber Deterrence an Illusory Course of Action? Journal of Strategic Security 7, no. 1 (2013): 54-67.

23. Rid and Buchanan, Attributing Cyber Attacks, The Journal of Strategic Studies, p. 31 available at: https://ridt.co/d/rid-buchanan-attributing-cyber-attacks.pdf

24. Bartholomew and Guerrero-Saade, Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks, 2016 available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf

25. Dr. Max Smeets, Cyber Deterrence Is Dead. Long Live Cyber Deterrence! CFR, February 18, 2020 available at: https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence,

26. JOSEPH S. NYE, JR, Deterrence in Cyberspace, Project Syndicate Jun 3, 2019.

27. Glaser, Charles, Deterrence of Cyber-attacks and US National Security, GW-CSPRI-2011-5. Washington, DC: Cyber Security Policy and Research Institute: 2, 2011.

28. P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar, Oxford University Press, 2014, pp. 144–146.

29. Kim Zetter, Senate Panel: 80 Percent of Cyber Attacks Preventable, Wired, November 17, 2009 available at: https://www.wired.com/2009/11/cyber-attacks-preventable/

30. China's Tech Trailblazers, Economist, August 6, 2016, p. 7 available at: https://www.economist.com/leaders/2016/08/06/chinas-tech-trailblazers

31. Quentin E. Hodgson, Logan Ma, Krystyna Marcinek, Karen Schwindt, Fighting Shadows in the Dark, Understanding and Countering Coercion in Cyberspace, RAND Corporation, 2019, available at: https://www.rand.org/pubs/research_reports/RR2961.html

32. Strategy, Joint Doctrine Note 2-19, 10 December 2019, available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn2_19.pdf?ver=2019-12-20-093655-890

33. Thomas C. Schelling, Arms and Influence, New Haven, Conn.: Yale University Press, 1966, available at: https://yalebooks.yale.edu/book/9780300143379/arms-and-influence

34. Quentin E. Hodgson, Logan Ma, Krystyna Marcinek, Karen Schwindt , Fighting Shadows in the Dark Understanding and Countering Coercion in Cyberspace, Rand Corporation Report available at: https://www.rand.org/pubs/research_reports/RR2961.html

35. National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience, Homeland Security, 2013 available at: https://www.dhs.gov/sites/default/files/publications/NationalInfrastructure-Protection-Plan-2013-508

36. Fischerkeller, Michael P. and Harknett, Richard J, Deterrence is Not a Credible Strategy for Cyberspace, Orbis, Vol. 61, Issue 3, 2017, 381-393.

37. Ibid

38. Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence (Department of Defense, February 2017) (www .acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport02-28-17Final.pdf).

39. Jeffrey W. Knopf, The Fourth Wave in Deterrence Research, Contemporary Security Policy 31, no. 1 (2010), pp. 1–33.

40. Erik Gartzke and Jon R. Lindsay, Thermonuclear Cyberwar, Journal of cybersecurity.

41. Jon r Lindsay and Erik Gartzke, Introduction: Cross-Domain Deterrence, From Practice to Theory, in Cross- Domain Deterrence: Strategy in an Era of Complexity, ed. Erik A. Gartzke and Jon r. Lindsay (Oxford: Oxford University Press, 2019), 6 available at: https://global.oup.com/academic/product/cross-domain-deterrence-9780190908645?cc=in&lang=en&

42. James C. Dawkins, 'rising Dragon: Deterring China in 2035': (Fort Belvoir, VA: Defense Technical Information Center, 12 February 2009), 12 available at: https://hcss.nl/sites/default/files/files/reports/Cross%20Domain%20Deterrence%20-%20Final_0.pdf

43. King Mallory, New Challenges in Cross-Domain Deterrence, Santa Monica: RAND Corporation, 2018 available at: https://www.rand.org/pubs/perspectives/PE259.html

44. Maj Gen PK Mallick, VSM (Retd), Social Media in Violent Conflicts – Recent Examples, Vivekananda International Foundation, August 2021 available at: https://www.vifindia.org/sites/default/files/Social-Media-in-Violent-Conflicts_0.pdf

45. Cyber Deterrence Is Dead. Long Live Cyber Deterrence! Council on Foreign Relations, February 18, 2020 available at: https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence

46. Erik Gartzke and Jon R. Lindsay, Thermonuclear Cyberwar, Journal of cybersecurity.

47. The Essence of Cross-Domain Deterrence, Tim Sweijs 1Email author Samuel Zilincik, The Hague Centre for Strategic StudiesThe HagueThe Netherlands 04 December 2020

48. Michael S. Chase and Arthur Chan, 'China's Evolving Approach to Integrated Strategic Deterrence', Product Page (Washington: RAND Corporation, 2016), vii. Chase, M. S. and Chan, Santa Monica, CA: RAND Corporation, available at: https://www.rand.org/pubs/research_reports/RR1366.html

49. Adamsky, Cross-Domain Coercion, 37 available at: https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf

50. Jason Healey, Not The Cyber Deterrence the united States Wants', Council on Foreign Relations (blog), June 2018 available at: https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants

51. Mason Richey, Contemporary Russian revisionism: understanding the Kremlin's Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation, Asia Europe Journal 16, no. 1, March 2018, 101–103 available at: https://link.springer.com/article/10.1007/s10308-017-0482-5?shared-article-renderer

52. Shawn Brimley, Promoting Security in Common Domains, The Washington Quarterly 33, no. 3, July 2010, 129 available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a536657.pdf

53. Juarez, '2015 Cross-Domain Deterrence Seminar Summary report', 2016, 6 available at: https://cgsr.llnl.gov/content/assets/docs/CDD_Report_Nov_2016_FINAL.pdf

54. Lewis, 'Cross-Domain Deterrence and Credible Threats', available at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100701_Cross_Domain_Deterrence.pdf

55. Tim Sweijs and Samo Zilincik , Cross Domain Deterrence and Hybrid Conflict, The Hague Centre for Strategic Studies, December 2019, Jon R. Lindsay and Erik Gartzke, "Cross-Domain Deterrence and Cybersecurity: The Consequences of Complexity," in US National Cybersecurity: International Politics, Concepts and Organization,edited by Damien van Puyvelde and Aaron F. Brantley (New York: Routledge, 2017). available at: https://hcss.nl/sites/default/files/files/reports/Cross%20Domain%20Deterrence%20-%20Final.pdf

56. Henry Farrell and Charles L. Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine," Journal of Cybersecurity 33, no. 1 (2017): 7–17 available at: https://academic.oup.com/cybersecurity/article/3/1/7/3074707

57. Report of the U.S. Defense Science Board (DSB) Task Force on Cyber Deterrence available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf

58. Senator Angus King, Cyberspace Solarium Commission, 11 Mar 2020 available at: https://www.solarium.gov/

59. Susan Hennessey, Deterring Cyber attacks How to Reduce Vulnerability, Foreign Affairs, November/December 2017 available at : https://www.foreignaffairs.com/reviews/review-essay/2017-10-16/deterring-cyberattacks

60. Colin Clark, Mandiant CTO: Cyber Attribution, Deterrence More Vital Than Defense, August 06, 2021 available at: https://breakingdefense.com/2021/08/mandiant-cto-cyber-attribution-deterrence-more-vital-than-defense/?utm_campaign=Breaking%20News&utm_medium=email&_hsmi=147326354&_hsenc=p2ANqtz8T

61. Michael Sulmeyer, How the U.S. Can Play Cyber-Offense Deterrence Isn't Enough, Foreign Affairs, March 22, 2018, available at: https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense

62. Robert Chesney, Sanctioning Russia for SolarWinds: What Normative Line Did Russia Cross? Lawfare, April 15, 2021 available at: https://www.lawfareblog.com/sanctioning-russia-solarwinds-what-normative-line-did-russia-cross

63. Zolan Kanno-Youngs and David E. Sanger, U.S. Accuses China of Hacking Microsoft, The New York Times, July 20, 2021 available at: https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html?campaign_id=60&emc=edit_na_20210719&instance_id=0&nl=breaking-news&ref=cta&regi_id=59331778&segment_id=63829&user_id=ec787ec8820f5d5fec4e77cc0682d1b1

64. Executive Order on Improving the Nation's Cybersecurity, The White House, MAY 12, 2021 available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

65. Clint Hinote, How to Stop the Next Hack Deterrence in Cyberspace, 04 January 2015 available at: https://www.foreignaffairs.com/articles/2015-01-04/how-stop-next-hack

66. Statement by President Donald J. Trump on the Elevation of Cyber Command, 18 August 2017, available at: https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/

67. Mariarosaria Taddeo, The Limits of Deterrence Theory in Cyberspace, Philosophy & Technology volume, 31, 339–355, 2018 available at: https://doi.org/10.1007/s13347-017-0290-2

68. Mariarosaria Taddeo, The Limits of Deterrence Theory in Cyberspace, Digital Ethics Lab, Oxford Internet Institute, University of Oxford, Alan Turing Institute.

69. Valeriano, Brandon, and Ryan C Maness, Cyber War Versus Cyber Realities: Cyber Conflict in the International System, Oxford University Press, . 2015, pp 57-60.

70. Ben Buchanan, The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations. Oxford: Oxford University Press, 2017.

71. Cliff Riggs, Network Perimeter Security. New York: Auerbach Publications, 2004.

72. Research Department of Military Strategy. The Science of Military Strategy, p. 134.

73. Dennis j. Blasko, Peace Through Strength": Deterrence in Chinese Military Doctrine, War on the Rocks, , March 15, 2017 available at: https://warontherocks.com/2017/03/peace-through-strength-deterrence-in-chinese-military-doctrine/

74. Ibid

75. Experts Analyze U.S. Network Deterrence Strategy: It Is Difficult to Achieve Real Results" (in Chinese), China News, January 9, 2012 (www .chinanews.com/gj/2012/01-09/3590771.shtml

76. Research Department of Military Strategy, The Science of Military Strategy.

77. Dean Cheng, Chinese Views on Deterrence, Joint Force Quarterly 60, no. 1 (2011),pp. 92–94.

78. Dean Cheng, Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC, Washington: Heritage Foundation, January 21, 2016 available at: www.heritage .org/research/reports/2016/01/prospects-for-extended-deterrence-in-space-and-cyber-the-case-of-the-prc

79. Adam Segal, An Expansive, and Dangerous, Chinese View on Cyber Deterrence, Council on Foreign Relations, January 25, 2016 available at: https://www.cfr.org/blog/expansive-and-dangerous-chinese-view-cyber-deterrence

80. Dean Cheng, Evolving Chinese Thinking About Deterrence: What the United States Must Understand About China and Space, Heritage Foundation, March 29, 2018.

81. Office of the Secretary of Defense, Annual Report to Congress, 2020, p. 88.

82. Michael Daniel, Closing the Gap: Expanding Cyber Deterrence, Global Commission on the Stability of Cyberspace (GCSC), The Hague Centre for Strategic Studies (HCSS). July 2021

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