ORF ISSUE BRIEF

NOVEMBER 2018
ISSUE NO. 266

The Impact of Cyber Warfare on Nuclear Deterrence: A Conceptual and Empirical Overview

KARTIK BOMMAKANTI

ABSTRACT Cyber war is a subject that is highly contested among strategists and experts. This brief assesses the impact of cyber operations against strategic targets and demonstrates that while cyber war is a real phenomenon, it is far from producing decisive outcomes. The cyberspace is a medium to conduct military operations and several countries have made investments in capabilities to both attack and defend against cyber-attacks. The brief evaluates the relative strengths of offence and defence and the extent to which it favours the strong against the weak. It considers whether cyber capabilities create asymmetric advantages, thereby undermining nuclear deterrence and strategic stability. The extensive use of cyberspace creates opportunities as well as challenges and vulnerabilities for countries that possess cyber capabilities.

(This brief is part of ORF's series, 'National Security'. Read the other papers in the series here: https://www.orfonline.org/series/national-security/)

INTRODUCTION

How do cyber operations affect nuclear deterrence and stability? While a fully satisfactory answer to this question might not be forthcoming, the subject does merit serious engagement. After all, the emergence of the cyber medium for warfare introduces a peculiar challenge for strategists. This brief unpacks the impact of cyber war on nuclear Command, Control and Communications (C3). How vulnerable would it render C3 systems and nuclear infrastructure and their delivery capabilities generally, thereby adversely affecting nuclear stability? The succeeding analysis maps out the key issues surrounding the cyber instrument in warfare. It also seeks to demonstrate the extent to which cyber

Observer Research Foundation (ORF) is a public policy think-tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research, and stimulating discussions. The Foundation is supported in its mission by a cross-section of India's leading public figures, academics, and business leaders.

To know more about ORF scan this code

ISBN: 978-93-88262-53-8

warfare could affect nuclear deterrence and strategic stability, if a state's Nuclear Command, Control and Communications (NC3) could be threatened or undermined. The management and safety of nuclear weapons is becoming increasingly dependent on computer systems, creating its own set of challenges. This brief argues that cyber weapons can threaten the stability of nuclear deterrence, but the outcome from cyber engagement might not be crippling to a country's nuclear capabilities.

Therefore, cyber operations are unlikely to be decisive on their own, but certainly damaging as cyber warfare tends to favour the strong over the weak.[1] There is another view, though, which holds that cyber warfare favours the weak over the strong. The reason for this alluring claim is that cyber operations are viewed as offense dominant bequeathing an asymmetric advantage to the weak making cyber defences more vulnerable. This is not entirely true, because strategic targets, integral to the focus of this brief are much harder to attack through the cyber medium than are more soft targets such as banking systems. Cyber defence by the strong can prevent attacks against critical infrastructure including power stations and military targets such as ballistic missiles, delivery platforms such as nuclear submarines and NC3 systems. Yet vulnerabilities of strategic capabilities have to be identified to be effectively exploited such as their complexity and configuration and a cyber-weapon has to be specifically created for each strategic target.[2] There is no single or generic cyber-weapon, which can be used against all critical infrastructure and strategic targets.[3]

They could render a victim if not outrightly defenceless, at least more vulnerable to pressures such as nuclear blackmail; they render inoperative NC3 and create conditions for an opponent to gain advantages elsewhere. Cyber operations can generate costs for nuclear command and control systems for a state against another. This brief is structured as follows: it first defines cyber weapons and clarifies the debates dividing the international strategic community over the occurrence and non-occurrence of cyber war. The second section then evaluates the impact of cyber warfare on nuclear deterrence and stability, and examines how cyber warfare can have a destabilising effect on nuclear deterrence. The brief closes by drawing attention to the implications of cyber warfare for India, and describing the consequences for stability in the South Asian region.

'CYBER WARFARE': DEFINITION AND OCCURRENCE

The first challenge in this analysis is in defining what "cyber" means. As Andrew Futter observed, "cyber is a fundamentally contested term" to the extent it cannot simply be treated as a synonym for the internet.[4] More specifically, "cyber" must be taken to mean as Martin Libicki defined it: "command and control of computers".[5] The *Merriam Webster Dictionary and Thesaurus* defines the word "cyber" as "of, relating to, or involving computers or computer networks (such as the internet).[6]This means that a computerised grid or a digitised grid is potentially susceptible to penetration. While a computer network connected to the internet is susceptible to attacks, computer networks that are not connected to the internet are also vulnerable if they get infected with malware. The latter targets are known as "air-gapped" networks in that they are not connected to the internet. Generally, any system connected to the internet is more vulnerable to attack than a system that is not. This will be discussed in more detail in latter parts of this brief; here it suffices to note that the interface between humans and machines is crucial to understanding the relative effectiveness against air-gapped strategic targets and critical infrastructure.

The other definition that must be made clear is that of a "cyber-weapon". In 2011, the Pentagon was hardpressed in defining a "cyber-weapon", claiming, "There is currently no international consensus regarding the definition of a 'çyber weapon'."[7] Thomas Rid instead defines a cyber-weapon as a subset of weapons more generally, specifically defining it: "as a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."[8] Cyber weapons are not very different from a conventional missile system. It has two parts: a delivery system and a payload. The former distributes the malicious code or the payload to various parts of a target machine and undertakes the task of installing the code.[9] The code then executes the actual attack, which could include stealing data, slowing down the operating speed of a machine, or destroying it altogether.[10]

Cyber weapons cover a spectrum of low- to high-end capabilities. The low-end cyber weapons, while generally of nuisance value—including software that disrupts traffic, denies service to users and temporarily slows down internet services—do not cause any enduring damage to any living being, structure or system. Low-end attacks can include defacement of websites and intellectual property theft; they could bring down the market value of a company if its online services are frequently disrupted by such incidents.[11] On the high-end of the spectrum are cyber weapons. They are designed to penetrate computer systems or an electronic grid. These are designed to take out particular targets.

Stuxnet malware is the most visible example of a high-end digital weapon specifically developed to damage centrifuges at Iran's Natanz facility. The malware can cause significant damage to industrial and strategic computers systems. Yet digital weapons such as *Stuxnet* are not only difficult to develop, they can also result in extensive, unintended damage if they fail to strike their intended target with precision.

There are two schools of thought that seek to debate about cyber war and whether or not it is occurring (or will occur). The first school says that cyber warfare will not occur, and nor is it occurring, and draws on Clausewitz's conception of war. First, this thought says, it lacks the violent character of war in that it is *not lethal*. Second, war is a means to a purposive end. Given its *instrumental* nature, war is geared to compel the enemy to do the attacker's will.[12] Cyber warfare does not meet this test. The third factor is *attribution*. War is never an isolated act; it is driven by intent and will. Generally, in war the opponent is known.

In the case of cyber-attacks, it is hard to ascertain the identity of the attacker. Since the possibilities of concealment are high in the digital domain, responding to cyber-attacks is fraught with difficulties.

Briefly, according to this school: "Any act of war has to have the potential to be lethal; it has to be instrumental; and it has to be political."[13] Cyber warfare does not meet these criteria. Cyber operations are therefore deemed more a criminal act than an act of war, fulfilling the three criteria of sabotage, espionage and subversion.[14] Sabotage involves damaging an economic or military system. According to this school, it is "predominantly technical in nature." It does not necessarily involve physical destruction or overt violence. Therefore, sabotage cannot be deemed an armed attack, because saboteurs do not claim attribution.[15] A second criterion for cyber-attack is espionage. It is deemed an offensive activity, albeit geared to penetrating the adversary's computer security and even disrupt their use of information. The empirical evidence, according to this school, suggests that espionage is more common in cyber security breaches. However, it is "not an act of war, not a weapon and not an armed attack". It is considered "a non-violent activity."

Lastly, the final offensive activity is subversion: it is geared to undermining an existing order. Within the cyber domain, it could have both positive and negative consequences. It is positive when an existing order is overly rigid and disrupted through technology "start-ups". There is also a negative to this: the cyber medium also provides political movements that have dangerous agendas to reorganise governments, if not overthrow as insurgencies are geared to doing. Further, the means used by subversives, according to this school are not always violent, rather directed towards undermining faith in a government and influencing undecided citizens to mobilise for a cause that could threaten the stability of a regime. These factors indicate that subversion in the cyber domain also lacks the violent character of war. However, subversive movements using the cyber domain might find it difficult to maintain organisational control.[16] For these reasons, this school argues that subversion is an offensive act, but not an act of war. Therefore, cyber war will not take place, because it simply lacks the destructiveness and the violence that characterise other forms of warfare.

On the other hand, the second school contends that cyber war will occur and is in fact already underway. The most well-known claims about the inevitability of cyber war were popularised by John Arquilla and David Ronfeldt as early as in the 1990s.[17] Subsequent to their publication, many other analysts have written extensively about the subject.[18]

It took a while before strategic experts came to grips with the potential damage of cyber-attacks. The promise and perils of cyber warfare are not unique *per se*. As Andrew Futter put it, "The security, safe storage, secure communication, and reliability of information have been intrinsic to national security and warfare throughout history. Equally, stealing, altering, and destroying key information; attacking, sabotaging, and compromising the means of storing and sharing this information;

and seeking to alter perceptions and policies through deception and psychological operations have always been a central part of warfare too."[19]

The emergence of the cyber domain of conflict is recent; cyber warfare against strategic targets had to be taken seriously given the levels of digitisation and computerisation that the world was experiencing. The extent to which critical infrastructure, including nuclear command and control systems, delivery systems and nuclear infrastructure are dependent on computer and electronic networks for their effective functioning and operation mandates policymakers to pay more attention to the adverse impact of cyber operations. It is in this context that a second school took issue with the first school that strategic thought is much too ambiguous about what constitutes war. They point to the conceptual tension between force, lethality and violence within strategic thought. Force need not be lethal to be violent in that it kills only humans; rather it could be confined to the destruction of inanimate objects such as infrastructure and other physical artefacts. As John Stone put it: "…cyber-attacks represent a particularly efficient means of translating force into violence: a few strokes are all that are required to set in train a sequence of potentially very violent events."[20] Even the US Department of Defence Law of Armed Conflict concedes that mass casualties could occur if the cyber-attacks were to: "1. Trigger a nuclear plant meltdown, 2. Open a dam over a populated area, causing destruction, or 3. Disable air traffic control services, resulting in airplane crashes."[21]

Elaborating further, this school contends that attribution need not be a criterion for whether or not cyber war will occur. It could involve attacks that are non-attributable, because "Clausewitz's definition of war", after all "as an act of force does not require that the act be claimed or attributable."[22]

Regardless of the issue of attribution, the empirical record over the last decade or so would confirm the occurrence of some form of cyber warfare. In any case, there is evidence to suggest that cyber-attacks are traceable and trackable despite the challenges to ascertaining the identity of the attacker quickly. Even so, a response to a cyber-attack is not always easy. The reason is simple: the cyber-attack may come from assume state A, which need not pursue cyber operations from its territory, it could potentially target state B, its adversary from a neutral state C and it could even go one step further by executing cyber operations from the territory of the target state B.[23] State A can also emplace hackers overseas to target state B.[24] This is where the challenge of non-attribution becomes relevant, not because there is no hostile intent behind state A's action against state B, but due to state B's inability to ascertain the source of attack.[25] This shows why deception and subterfuge are integral to cyber operations and cyber war as they are with other forms of warfare.

Non-attribution may create constraints or be an advantage in some instances. Without discounting the effect of intangible factors such as uncertainty, friction and chance in war,[26] as one expert put it: "With proper planning and execution, non-attributable effects are possible in every war-fighting domain. There is diversity in non-attributable effects. It can be cognitive, logical, or physical in nature. In this sense, non-attributable effects might include covert aerial drone strikes, difficult-to-trace offensive cyberattacks…"[27] Concealment also plays an important part in this medium of warfare. Despite the importance of the second school's claim about non-attribution, attribution or at least the identity of the source of attack is a necessity if the adversary is to retaliate against an attack. After all, Clausewitz's definition of war also characterises war as a collision between two or more opposing wills and a contest of arms between animate entities.[28] As Clausewitz notes: "War…is not the action of a living force upon a lifeless mass (total non-resistance would be no be no war at all) but always the collision of two opposing forces. The ultimate aim of waging war, as formulated here, must be taken as applying to both sides."[29] Consequently, the defender has to know the source of attack to respond even if it is delayed retaliation; otherwise, it would not be war at all.

When taken as a whole, the second school may be more accurate in concluding that cyberwar will occur, with the qualification that attribution is a necessary but insufficient condition. However, the question is in relation to the scope and extent of damage that cyber operations can inflict on an opponent's military capabilities, critical infrastructure and nuclear command and control architecture, and the retaliatory measures taken by the defender or target. A corollary to this key question is another: what happens in cases where the opponent does not wield any cyber capabilities to retaliate, but discovers the source of attack? This brings the conversation to cross-domain deterrence and retaliation.[30] The initiator of an attack pursues it in one sub-domain such as cyberspace, and the target discovers the source attack and retaliates in another.

The target or opponent may respond in one of two ways—either escalate in another area where the state in question wields some relative advantage, or wield capabilities and opportunities to impose costs in the domain. One good example would be if state X, the victim of a cyber-attack from state Y, escalates through terrorist strikes where it wields tactical advantages as opposed to the cyber domain where it wields limited cyber capabilities, if at all. This would count as cross-domain deterrence in that the threat or actual retaliation occurs not within the domain of attack (example: cyberspace), but occurs in another domain such as sub-conventional sub-area.[31]

As Lawrence Freedman observed: "Even if a strategic information campaign could be designed and mounted, there could be no guarantee that a victim would respond in kind, rather than with whatever means happened to be available."[32]

To be sure, notwithstanding the fact that cyber warfare is not exclusively about the conduct of a "strategic information campaign" but the use of the digital medium to cause physical damage to the opponent's strategic and critical infrastructure as was seen with the *Stuxnet* attack and Iran's cyber response to *Stuxnet*. However, it could also be a medium to deny an opponent access to information, particularly in the course of war, thereby gaining an upper hand in military operations or access to critical assets during a crisis. Beyond being purely disruptive as is often understood by Information Warfare (IW), cyber operations encompass the entire gamut of missions that could potentially alter, corrupt and delete information.[33]

Nevertheless, Freedman is accurate in noting that a state, which is the victim of a cyber-attack, might not respond in kind. This is where cyberwar is analogous with other forms of warfare. It is not difficult to come by an illustrative example in the subcontinent. The India-Pakistan wars provide examples of states not fighting according to each other's terms. For instance, in 1965 following the Pakistani attack in Jammu and Kashmir across the ceasefire line, India retaliated with a counter offensive across the International Border (IB). The Pakistanis did not expect an Indian counter offensive across the IB. Another example is the Kargil conflict in 1999 where, following the Pakistani attack, India escalated vertically with ferocity using airpower, taking the Pakistanis by surprise.

The opposite also holds true: India faces Pakistani terrorism, but does not respond in kind. Indians cannot assume Pakistan is going to fight exclusively on Indian terms. However, it is more plausible for a state such as China to respond in kind with a cyber-attack or potentially mount cyber operations in conjunction with other military instruments such as air, land, sea, and space power. On the other hand, the target state in question might not respond, because it has no means to do so or deems the cyber medium to be inadequate for a response. Nevertheless, cyber war is a real phenomenon and its impact on nuclear stability can be adverse and dangerous. If strategic stability breaks down because of cyber-attacks, it could trigger miscalculations and escalation. This brings the brief to the question of the impact of cyber warfare on nuclear stability.

THE CONSEQUENCES OF CYBER WAR ON NUCLEAR STABILITY: THE IMPORTANCE OF RIVALRY AND RELATIVE POWER

Given the foregoing, what is the relationship between cyber war and nuclear deterrence? Cyber operations can inflict blows against an opponent's NC3 capabilities rendering it, if not outrightly helpless, weakened and susceptible to coercion. Targeting a state's nuclear capabilities is a function of rivalry and relative power. The NC3 system and critical nuclear weapons infrastructure is potentially susceptible to computer malware penetration. Any network connected to the internet is highly vulnerable to attack. However, states can and presumably do take measures to insulate their nuclear infrastructure and NC3 system by de-linking or “air-gapping” their electronic and computer networks from attacks.[34] To be sure, air-gapping at best mitigates vulnerabilities to systems, enabling better cyber-defence; however, potential adversaries can breach these security firewalls through external devices.

In these cases, the Human-Machine Interface (HMI) is crucial to whether the cyber operations are effective. HMI related infections can manifest in two distinct ways. The first is through the introduction of a memory stick infected with a cyber-weapon and inserted by a human into a computer network. The second is potentially through an insider threat. Human threats within an organisation and command systems that oversee weapons systems and personnel could be potentially compromised and sabotaged. See for instance Table 1, which captures the vulnerabilities to nuclear capabilities in the form of *enabling* and *disabling* factors, corresponding with *positive* and *negative* nuclear command and controls.[35] Beginning with the latter, *disabling* attacks cover jamming and interference with communication "go codes" retarding, compromising and preventing transmission to weapons systems. Negative controls are geared to prevent nuclear use and *disabling* attacks are aimed to undermine it through spoofing early warning systems, radar and satellites. On the other hand, the *positive* side of nuclear controls are designed to ensure actual nuclear use. Hackers may actually facilitate nuclear launches by spoofing early warning system into assuming that nuclear attacks were underway, when none is. This could be accomplished through *enabling* attacks by undermining procedures and mechanisms by hacking into plans, programmes and launch control systems.[36]

The most prominent example of how cyber operations can retard a country's nuclear programme was the joint US-Israeli cyber operation using the *Stuxnet* virus on the Iranian nuclear programme and nuclear command systems. *Stuxnet* was a product of the HMI. It involved a human machine interface whereby the virus itself was implanted using a flash drive by human agents.[37] *Stuxnet* targeted the critical nuclear infrastructure of Iran and not Tehran's NC3 capacities. The virus struck Iran's gas centrifuges in the Natanz nuclear facility that were crucial to the country's nuclear enrichment programme. *Stuxnet* is considered

Table 1. Vulnerability of Nuclear Command and Control Systems

Enabling - positive controls	***Disabling – negative controls***
A Direct hack in the command and control systems	Sabotage weapons systems.
Issue "go codes" to weapons system and nuclear commanders	Jam communications and early warning systems, disabling them -- orders cannot be received and commanders are left confused.
Dissimulate or mislead early warning systems into believing that a nuclear attack is underway. Distort the nuclear information space.	Weaken nuclear systems by stealing information on how they work.
Use terrorist proxies and other non-state actors.	State-based actors are likely to pursue such attacks.

Source: Adapted from Andrew Futter, 'Hacking the Bomb: Cyber Threats and Nuclear Weapons', 2018, p. 49 "the most technologically sophisticated malicious program developed for targeted attack"[38] and a "guided cyber missile".[39] *Stuxnet* was a worm whose origins were in the digital world that wreaked damage in the physical world.[40] It is also without precedent and widely considered a destructive cyber-attack, against a high-value military target even by those who do not subscribe to the view that cyber war will happen.[41] A careful look at how the process played out reveals that it took considerable planning and preparation gleaned from intelligence gathered over several years. It started first with an International Atomic Energy Agency (IAEA) inspection of the Natanz nuclear facility in February 2003, where Tehran planned to install 1,000 centrifuges by the end of the same year.[42] The IAEA inspection regime required that Iran hand over details about the installation of new equipment such as valves, machine tools and vacuum pumps. Western intelligence had been monitoring where Iran procured equipment in secrecy. The Neda Industrial Group, an industrial firm, acquired equipment on behalf of the Iranian nuclear programme. The company collaborated with Kalaya Electric Company, which was transformed into a centrifuge manufacturing plant.[43] The Neda group was also a domestic partner of the German company Siemens, which supplied the S7 Programmable Logic Controller (PLC). Siemens supplied PLCs for a range of other industrial activities in Iran.[44] For a simplified version of how PLCs generally operate, see images 1 and 2.

Investigators found that Siemens-supplied PLCs were a crucial piece of intelligence that

Image 1 – A Basic PLC Configuration

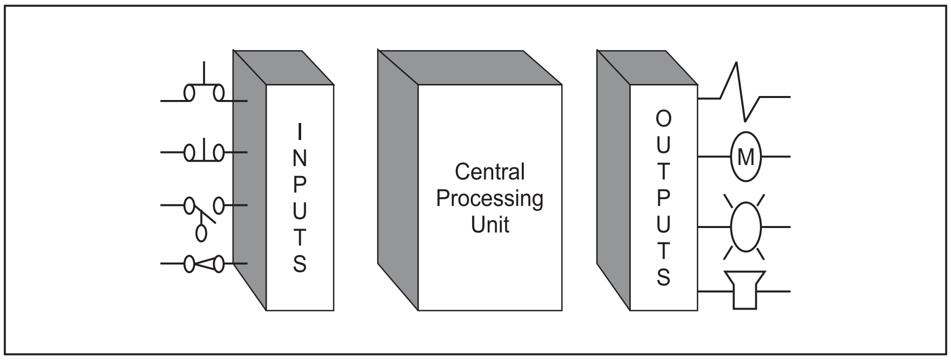
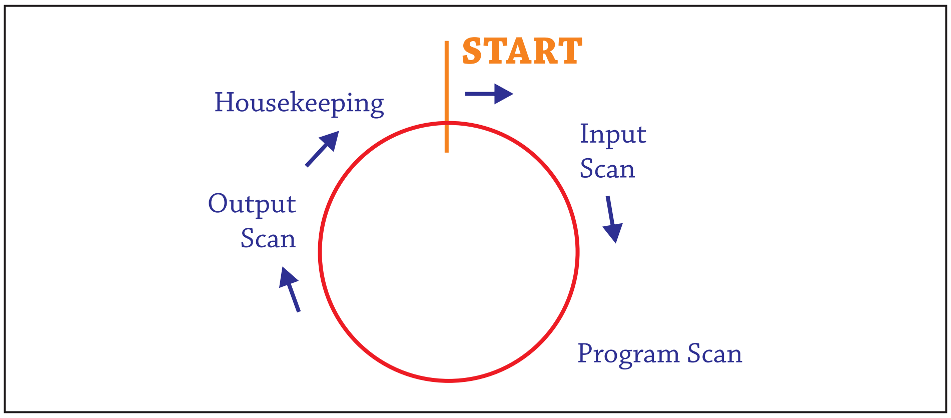


Image - 2



enabled the planners of *Stuxnet* in Israeli and US intelligence to infer, given the fact that the same PLCs were installed for a range of other Iranian industrial activities. Iran's centrifuge facility at Natanz too used Siemens PLCs. *Stuxnet*, an autonomous worm, was implanted by human agents through a flash drive into a computer or a network of computers located at the site. It was designed to degrade Iran's enrichment capacity, rather than destroy it, including the gas centrifuges necessary to sustain enrichment.[45] It was a substantial collaborative operation involving the National Security Agency (US), the Central Intelligence Agency (CIA) and an elite unit of the of the Israeli intelligence dubbed 8200,[46] consisting of a cohesive and well-trained network of human spies. It demonstrates the importance of Human Intelligence (HUMINT) in a field that mandates high technical proficiency in penetrating the air-gapped nuclear infrastructure of the target state.

The foregoing description reveals the herculean challenge in the design and eventual use of *Stuxnet* for even the most formidable cyber powers. Nevertheless, cyber warfare suits the strong simply because they have the access, intent and time. As Thomas Rid observes: “Only very few sophisticated strategic actors may be able to pull of large-scale sustained computer sabotage operations.”[47]

That apart, when considering the development and employment of cyber weapons such as *Stuxnet*, it needs to be underlined that the state of political and strategic relations between states is the most consequential determinant for the conduct of cyber warfare. Only a pre-existing rivalry is the likeliest source of cyber war – a stipulation or condition that is missed by some, if not all cyber-war advocates. Further, *Stuxnet* and malware that matches its sophistication, are as much a product of relative power in that the stronger power has advantages. To be sure, the stronger power needs to integrate cyber warfare capabilities with doctrine, organisation, training, strategy and importantly understand the strength and the limits of cyber military technology. Otherwise, it runs the risk of inappropriately and erroneously applying and executing cyber offensives.

The cyber weapon *Stuxnet* was specifically used against Iran, a state locked in an irreconcilably hostile relationship with the United States and Israel. It was also used with great precision against a strategic target. As then Iranian President Mahmood Ahmadinejad said, “they succeeded in creating problems for a limited number of our centrifuges with the software they had installed on electronic parts.”[48] It also explains why strategic cyber war is most likely between two states locked in a conflict dyad riven by deep hostilities and antagonism. In August 2012, the Iranians did react to the *Stuxnet* attack by striking back at an American bank and one of Washington's closest regional allies, Saudi Arabia, subjecting its state-owned oil giant ARAMCO to cyber-attacks by partially replicating *Stuxnet*.[49] As a US National Security Agency (NSA) analysis put it: “Iran's destructive attack against Saudi ARAMCO in August 2012, during which data was destroyed on tens of thousands of computers, was the first such attack NSA has observed from this adversary."[50] To be sure, Iran's cyber response known as *Shamoon*, a malware, inflicted damage on the Saudi oil sector. Oil exports are a critical source of revenue for the Saudi economy. Notably, Iran's response was not geared to retaliating against the American and Israeli nuclear programmes, but the American banking system, which is considered a soft target. Even in this case, the execution of the attack was amateurish, causing nuisance with damage done at most to the denial of internet service to the customers of the targeted American banks.[51]

This point is crucial, as observed earlier, because the differential in the nature of the targets pursued by Israel and the US, on the one hand, and Iran's response, on the other, reflects the relative power balance between the adversaries. The Israelis and the Americans targeted Iran's nuclear programme – a high-value strategic target, whereas Iran was at best able to do damage of some kind to Saudi Arabia's oil giant Aramco and some American banks.

Iran's response on the other hand, while inflicting damage, only struck American banks and Washington's ally in the region, while they remained unscathed from Iran's response. Although the latter is a critical target, it pales in comparison to the sophistication and planning involved in targeting Iran's centrifuge programme. As Colin Gray wrote, "War is politics, and politics is about relative power."[52] This statement is instructive, because the joint US-Israeli cyber-attack against Iran's nuclear centrifuges was a highly sophisticated attack involving dedicated teamwork and a joint effort against a high-value target: Tehran's nuclear sector. One reality that should not be underestimated is that cyber-attacks are not easy against highly secure targets such as the nuclear and space programmes of states in the advanced industrialised world. *Stuxnet*-like malware take time to plan and engineer for effective use against an adversary. Based on all the evidence available in the public domain, cyber warfare planners are compelled to collect intelligence on the "mechanical and physical" characteristics of their targets. *Stuxnet* was precisely such a cyber-weapon that required considerable engineering skill and long preparation, and even when it did successfully attack Iran's centrifuges, it only set it back by at best a year.[53]

To be sure, the weaker power, which is the target of a cyber-attack, may respond, but its counter cyber-attacks may be ineffective either due to the lack of sufficient cyber strength or due to the robust defences prepared by the defender.[54] On the other hand, should a weaker power initiate attack, Thomas Mahnken observes, "The weaker power might be able to cause a stronger power some annoyance through cyber-attack, but seeking to compel an adversary through cyber war, it would run the very real risk of devastating retaliation."[55] Although some might qualify this by noting that the strong do not have an outright advantage in the cyber domain, they do wield a relative advantage over the weak and defence is stronger than presumed by advocates of the "Cyber Revolution" thesis.[56] Yet offence dominance is hard to attain in the cyber realm because cyber weapons are not easy to master, objectives are difficult to attain especially against strategic targets, and the potential for retaliation is real, if the adversary too fields potent cyber warfare capabilities.

These factors indicate the reason for the relative absence of cyber war; the offence is not significantly stronger than defence in the cyber domain.[57] Cyber-attacks are more daunting against high-value strategic infrastructure such as NC3 and nuclear infrastructure that host nuclear weapon systems.[58] Therefore, the possibility of cyber defense is high, when critical nuclear infrastructure and states NC3 architecture is taken off-line and air-gapped.[59] A non-internet-based digitised or computerised grid is harder to penetrate. When this is the case, a network of human spies becomes critical in penetrating digitised, electronic or computerised network as was the case that enabled the Stuxnet attack against the Natanz centrifuge facility.[60]

Further, the advantages of the strong are in preparing defences against attack and making post-attack recovery more rapid.[61] The technical demands of cyber warfare are such that the weak have limited capacities, which include technical and financial resources. These attributes mean that the weak are unlikely to wield the advantages of the strong. In the cyber domain, there are no substantial asymmetric advantages that the weak wield against the strong. At best, they may be able to sustain cyber-attacks against low-value or soft targets with low-end capabilities. As Lindsay observed, "Cyber warfare is not a weapon of the weak".[62] On balance, this statement is empirically valid. There are literally no cases where the weak have inflicted considerable pain against the strong. *Stuxnet* was a cyber-weapon developed by the strong against the weak. Comparable responses and attacks similar to *Stuxnet* by the weak against the strong are absent. In a single day, hundreds of cyber-attacks, at a minimum, occur. Two or three of them, at most, may involve serious breaches of security, such as data theft and financial embezzlement. Yet serious strategic cyber-attack targeting C3 nuclear capabilities are still rare and ultimately a capacity only the strongest cyber powers will possess at least for the near future. Even more, the weak have not yet demonstrated a comparable capacity for imposing losses against the strong's strategic facilities and critical infrastructure.

Briefly, cyber war, if not always, generally favours the strong against the weak. Indeed, three features of cyber threat that the strong

Table 2 Nature of the Cyber Threat

Capability	Talent, time and money to generate an adverse effect against the target.
Access	Remote or physical access to the target system, or access-less, and
Intent	The drive to pursue cyber operations, which is presumed to exist.

Source: Adapted from Kamal T. Jabbour and Erich Devendorf, "Cyber Threat Characterization", The Cyber Defence Review, Vol.2, No. 3 (Fall 2017), p. 80 are likely to benefit from are capability, access and intent. (See Table 2). As noted earlier, there are significant technical demands on successfully prosecuting cyber warfare. The basis of information warfare is substantial availability of talent, time and financial resources.[63] Mathematical education provides the basis for Information theory, signals communications and encryption to conduct cyber warfare.[64] This is unlike other domains of warfare. A state such as China has a large number of institutions that provide the requisite talent pool and resources to cater to the requirements of cyber warfare.[65]

IMPLICATIONS FOR INDIA

While there may be multiple actors hostile to India, the most prominent will be state actors when it comes to threats to the Indian nuclear deterrent and, more generally, the civilian elements of its nuclear infrastructure. The states that come to mind immediately are China and Pakistan – between these two states, the former is likely to present the most potent cyber military threat to its nuclear C3 capabilities. Chinese cyber capabilities are integrated with its electronic and psychological operations capabilities as part of the Network Systems Department (NSD).[66] China wields potent offensive cyber warfare capabilities. In the Sino-Indian conflict dyad, China is the superior power simply because of the human and technical resources it possesses. Attention to cyber military issues should gather greater urgency for the Government of India (GoI) as Beijing has already demonstrated a capacity to penetrate some of India's most consequential capabilities such its missile systems.[67] Beijing has also shown that it can perpetrate repeated cyber-attacks against critical Indian government departments such as the Ministry of Defence.[68]

This is simply a function of the material capacities of the Chinese state. The greater challenge for India is collusion between China and Pakistan to disable India's nuclear C3 systems, given the conflictual and competitive relations between India on the one hand, and China and Pakistan on the other. India also faces the crucial test of preventing cyber-attack against civilian nuclear infrastructure such as power stations. Preparing the Indian state against cyber-attacks from China and Pakistan will require considerable investments in the security of its nuclear weapons, its command structure, and creating safety nets against potential attacks. In order to deter cyber war against its strategic assets and in the event deterrence collapses, there are three key areas where India will need investment focus: resilience, denial, and cyber offensive capabilities. An assured response is what India needs, which is geared towards both negative and positive aims. Resilience and denial are intended to meet negative or defensive objectives, whereas cyber offensive capabilities are geared towards positive or offensive objectives, which requires India's cyber capacities to strike at the adversary's high-value or strategic targets.

The protection of Indian arsenal as well as the C3 structure will require measures that dispense with digitised means of C3. Since the cyber medium is another means of war, inadequate investment in cyber defence capabilities against a technologically advanced foe such as China could prove deadly for India. Indian strategic planners must view cyber capabilities as a force multiplier, in that it can enable other modes of warfare particularly in the conventional domain. India will have to develop cyber capabilities for defence and attack. However, while cyber weapons can produce a damaging effect, they cannot generate a decisive outcome unless they are used in concert with other instruments of power. ORF

ABOUT THE AUTHOR

Kartik Bommakanti is an Associate Fellow with ORF's Strategic Studies Programme.

ENDNOTES

1. Multiple scholars and experts concur on this point. Thomas Rid, *Cyber War Will Not Take place*, (London: Hurst&Company, 2017), p. 168. See also Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies*, Vol. 22, Issue 3, pp. 394-398.
2. Rid, *Cyber War Will Not Take Place*, p. 168.
3. Ibid.
4. Andrew Futter, "Is Trident safe from cyber attack?" *European Leadership Network*, February 2016, https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/Is-Trident-safe-from-cyber-attack-1.pdf.
5. Cited in Futter, "Is Trident safe from cyber attack?", pp. 1-2.
6. See "Cyber" definition in *Merriam-Webster*, https://www.merriam-webster.com/dictionary/cyber.
7. Cited in Thomas Rid, *Cyber War Will Not Take Place*, (London: Hurst&Company, 2017), p. 37.
8. Ibid.
9. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, (New York; Broadway Books, 2014), p. 52.
10. Ibid.
11. Rid, *Cyber War Will Not Take Place*, p. 40.
12. Carl Von Clausewitz, *On War*, Michael Howard and Peter Paret (eds. and Trans.), (Princeton: NJ, Alfred A. Knopf, 1993), pp. 83-87.
13. Thomas Rid, "Cyber War Will Not Take Place", *The Journal of Strategic Studies*, Vol. 35, No. 1, February 2012, p. 6.
14. Ibid, pp. 16-26.
15. Thomas Rid, *Cyber War Will Not Take Place*, pp. 56-58.
16. Ibid, p. 113-138.
17. John Arquilla and David Ronfeldt, "Cyberwar is coming!", *Comparative Strategy*, 12/2, 1993, pp. 141.
18. For most recent see Martin C. Libicki, *Cyber Deterrence and Cyberwar*, RAND Report FA7014-06-C-001 (Santa Monica, CA: RAND, 2009).
19. Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons* (Washington DC, Georgetown University Press, 2018), p. 19.
20. John Stone, "Cyber War Will Take Place!", *The Journal of Strategic Studies*, Vol. 36, No. 1, p. 107.
21. Department of Defense Law of War Manual, *Cyber Operations and Jus ad Bellum*, (Washington D.C: Government Printing Office, 2016), https://www.defense.gov/Portals/1/Documents/pubs/

DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

22. Ibid, p. 105. See also Clausewitz, *On War*, pp. 83-101.

23. Martin C. Libicki, *Crisis and Escalation in Cyberspace*, (Santa Monica: CA, RAND Corporation, 2012), p. 127 (accessed from JSTOR).

24. Ibid.

25. See Jan Kallberg and Steven Rowlen, "African Nations as proxies in covert cyber operations", *African Security Review*, 2014, pp. 2-4.

26. Carl Von Clausewitz, *On War*, Michael Howard and Peter Paret (ed. and Trans.), (London: Alfred A. Knopf, 1993), p. 96-140.

27. Lt. Col. Garry S. Floyd Jr. USAF, "Attribution and Operational Art: Implications for Competing in Time", *Strategic Studies Quarterly*, Vol. 12, No. 2, Summer 2018, pp. 18-19.

28. Clausewitz, *On War*, p. 86.

29. Ibid.

30. King Mallory, "New Challenges in Cross-Domain Deterrence", Perspective, (Santa Monica: CA, RAND Corporation, 2018) pp. 3-10, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE259/RAND_PE259.pdf.

31. King Mallory, "New Challenges in Cross-Domain Deterrence", *Perspectives*, (Santa Monica, CA: RAND Corporation, 2018), pp. 1-17, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE259/RAND_PE259.pdf.

32. Lawrence Freedman, *The Revolution in Strategic Affairs*, (London: International Institute of Strategic Studies, 1998), p. 57.

33. Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, (Washington DC, Georgetown University Press, 2018), p. 21.

34. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, (New York: Broadway Books, 2014), p. 148.

35. Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, pp. 48-49.

36. Ibid.

37. Rid, *Cyber War Will Not Take Place*, pp. 43-45.

38. Aleksandr Matrosov, Eugene Rodionov, David Harley and Juraj Malcho, "Stuxnet under the Microscope", ESET, White Paper, 20 January 2011.

39. Mark Clayton, "Stuxnet Malware is "weapon" out to destroy…Iran's Bushehr nuclear plant", *Christian Science Monitor*, 21 September, 2010, https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.

40. Ibid.

41. Rid, *Cyber War will Not Take Place*, p. 32.

42. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World First Digital Weapon*, pp. 311-313.

43. Ibid.

44. Ibid.

45. Jon Lindsay, "Stuxnet and the Limits of Cyber Warfare", p. 391.

46. Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, (New York: Simon & Schuster Paperbacks, 2016), p. 205.

47. Rid, *Cyber War Will Not Take Place*, p. 169.

48. Cited in "Iran Says cyber foes caused centrifuge problems", *Reuters*, 29 November, 2010, <https://www.reuters.com/article/iran-ahmadinejad-computers-idAFLDE6AS1L120101129.

49. Kim Zetter, "The NSA Acknowledges What We All Feared: Iran Learns From US Cyber Attacks", *Wired*, 10 February, 2015 accessible at https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/.

50. Ibid.

51. Lindsay, “Stuxnet and the Limits of Cyber Warfare”, p. 397. See also Ellen Nakashima, “Iran Blamed for cyber attacks on U.S. banks and companies”, *Washington Post*, 21 September, 2012, lhttps://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html? utm_term=.069eeddc6852.

52. Colin S. Gray, *Another Bloody Century: Future Warfare*, (London: Weidenfeld and Nicholson, 2005), p. 64.

53. David Albright, Paul Brannan, Andrea Stricker, Christina Walrond, and Houston Wood, “Preventing Iran From Getting Nuclear Weapons: Constraining Its Future Nuclear Options”, The Institute for Science and International Security, 5 March, 2012, p. 15 https://isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf.

54. Jon Lindsay, "Stuxnet and the Limits of Cyber Warfare", pp. 395-402.

55. Thomas Mahnken, “Cyber War Favors the Strong”, Center for a New American Century”, Washington D.C., 11 June, 2018, accessible at https://www.cnas.org/press/in-the-news/mahnken-cyber-warfare-favors-the-strong.

56. Jon Lindsay, “Stuxnet and the Limits of Cyber Warfare”, *Security Studies*, Vol. 22. Issue 3, 2013, pp. 388.

57. Ibid, p. 395.

58. Ibid, p. 393.

59. See Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, (New York, NY: Simon&Schuster, 2016), p. 206.

60. Ibid, pp. 206-207.

61. Ibid.

62. Ibid, p. 389.

63. Kamal T. Jabbour and Erich Devendorf, “Cyber Threat Characterization”, *Cyber Defense Review*, Vol. 2, No. 3, Fall 2017, pp. 80-81.

64. Ibid, pp. 83-84.

65. Ibid.

66. Elsa B. Kania and John K. Costello, “The Strategic Support Force and the Future of Chinese Information Operations”, *The Cyber Defense Review*, Vol. 3, No. 1, Spring 2018, pp. 105-122.

67. Tania Branigan, “Cyber-spies based in China target Indian government and Dalai Lama”, *The Guardian*, 6 April 2010, https://www.theguardian.com/technology/2010/apr/06/cyber-spies-china-target-india.

68. Anil Anthony, “Repeated Cyber attacks ominous for a post-demonetisation India”, *Hindustan Times*, 12 June, 2017, https://www.hindustantimes.com/editorials/repeated-cyber-attacks-ominous-for-a-post-demonetisation-india/story-j55MpxtbEl99FRtLg21gBM.html.

ORF OBSERVER RESEARCH FOUNDATION
Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-35332000, Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org