# THE AGE OF CYBER WARFARE: UNDERSTANDING THE CYBER CONFLICT COMPLEX

**KHYATI SINGH**

Although the hype around cyber has reached a new height in the recent times, it is not a new entrant in the international domain. The link among cyber space, national security and technology existed in different ways. States have been targeting the systems of their enemy to extract crucial information and steal data, along with contesting the digital control of many national functions. Improvement and advancement in technology have also shaped the course of cyber conflict.

Cyber conflict has appeared on the surface, amounting to regional rivalry, hegemonic strategic gains, or for the sheer reason of national interest. The range of conflict varies from a spectrum of adversaries like unauthorised access, physical disruption, sabotage, espionage, and digital data theft to money laundering. Though, states are constantly engaged in cyber attacks and hacking, yet they have managed to operate below the threshold of conventional 'warfare' in terms of cyber. Before we dwell on the details of what unfolded in the cyber history, it is crucial to understand the nuances present in the term today. There has been slight discontentment over the synonymous use of the terms cyber conflict and cyber war. Just like not every activity across the border is war, not every miscalculation in cyber

Ms **Khyati Singh** is Research Associate at the Centre for Air Power Studies, New Delhi.

**Scholars refer to cyber conflict as actions between two players, either state or non-state, that develop a non-harmonious tone. This encompasses the deployment of malware to extract data, intelligence exploitation techniques and unauthorised access, along with other activities of this nature.**

space is cyber war. It is merely a conflict. Generally, scholars refer to cyber conflict as actions between two players, either state or non-state, that develop a non-harmonious tone. This encompasses the deployment of malware to extract data, intelligence exploitation techniques and unauthorised access, along with other activities of this nature. However, on the contrary, cyber war, much like a generic war, is used to refer to an episode where two politically recognised factions are in a tussle with one another via the cyber space. In a majority of cases, this comprises a hostile engagement with the sheer intention of wreaking havoc on the other. These politically recognised bodies are not necessarily states, but also involve terror groups, or other such non-state bodies. Moonlight Maze has been dubbed as the classic example of a cyber war.

Unlike a nuclear war which is direct and monolithic in its form, where nuclear exchange inflicts massive destruction, the case for cyber war is different. The idea generally is to extract information and refrain from engaging in what can be considered as aggression as per the traditional standards of state policy. Nevertheless, this does not rule out the possibility of massive disruption and physical damage that a cyber war causes. For instance, an attack on critical infrastructure, national energy grids, etc could lead to a wide range of distress and inadvertent deaths as well as monetary damage.

It is no wonder that any general inspection of cyber history will take into account the actions of the great powers because it was these advanced nations that deployed major resources to cyber war-fighting abilities. It has been the inherent nature of the international domain that the majority of the leads and advancements are kindled by the great powers, and it is this risk factor that also helps them maintain their status of great power. Hence, this is a two-way stream. Likewise, because these states chose the technical path, they stand more vulnerable to attacks as their system is entirely knitted around the technological user interface, unlike for smaller nations where such advancement has not percolated deep. In addition, inter-state conflict that has managed to reach the stage of modern cyber conflict has been limited in the international domain—the reasons for this could be numerous but the most pertinent has been that the cyber advances have not reached all states alike. If an attacker has offensive capabilities but its target is rooted majorly in the non-technical space, then the cyber conflict will not unleash maximum damage.

**If an attacker has offensive capabilities but its target is rooted majorly in the non-technical space, then the cyber conflict will not unleash maximum damage.**

The cyber conflict between states has essentially been conducted in four principal ways, and each of them has a unique set of characteristics in favour of the attacker.

First, '**Direct Disruption**,' or degradation attacking the core foreign security assets of a country.[1] Stuxnet is the prime example of this kind of attack wherein a state deployed digital capability to destroy the physical operation of a crucial facility. The common thread that runs in such operations is that they generally employ a malicious code to gain a visible disruptive outcome. They refrain from relying on secondary support arising from traditional military means to inflict tremendous damage. In addition, they target the facility of a specific security entity and can use means like physically damaging infrastructure. However, these attacks, have till now been limited to a specific target, but they can expand into multiple systems targets, and an entire country can also be targeted. This kind of operation is called cyber blockade.[2] In such an event, the entire national system is disconnected from the internet. This is achieved through massive denial attacks used against a state's set of Internet Service Providers (ISPs) in sync

[1] Brandon Valeriano, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford: Oxford University Press, 2018).

[2] Alison Russell, *Cyber Blockades* (Washington DC: Georgetown University Press, 2014).

with a range of complementary attacks on critical information infrastructure and critical regulatory systems. However, these blockade episodes are rare and shortlived mainly because they require enormous resources.

This does not entail that all cyber attacks are aimed at massive destruction—many of them aim to curtail the function of the opponent's capabilities, along with forestalling effective deployment of security assets, etc. This is the main line of differentiation between disruption and degradation. While one is aimed at strong damage, the other is largely meant to reduce functional efficiency.

This leads us to the next principal attack, namely, '**Enabling Attacks**.' Such attacks enable military operations; hence, they are mostly in a supporting role.[3] For instance, they can be used to target a small section of a particular national security system which, in turn, makes space for traditional military operations to take place.

The next in line is '**Manipulation of Information**,' cyber attacks that are aimed at dismantling the information environment in which political narratives, debates and policies are constructed. In such attacks, the cyber operations are composed of a series of actions designed to gain, reformulate, redirect, manipulate and modify the information to trigger a specific response from the society. These kinds of attacks are a common feature in democratic states because of their direct link with public opinion. The infamous episode of Russia's efforts to manipulate the political dialogue in the United States in 2016 is a textbook example of such attacks. This, when conducted on a larger scale, and with more extensive resources, translates into information warfare, where cyber merely becomes a tool to achieve the desired ends. Cyber actions are used to increase the functionality of non-cyber instruments like the conventional propaganda machinery. In addition, information dismantling attacks are also used to support domestic anti-national elements or international terrorist actors with a similar agenda. Likewise, data manipulation or cyber vandalism is another such way where

[3] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, 2013. Accessed on February 25, 2023.

the information is modified to introduce chaos into the system, and alter the shape of the public discourse. What citizens constantly consume in the mainstream channels is a tactfully designed syllabus to serve a particular narrative.

Lastly, '**Information Exfiltration**,' attacks that are continuous and coordinated attacks that span over years. They silently monitor information within the government network, industrial systems and military bases or steal information for a particular agency or government. This information is then exploited to make diplomatic gains, change the foreign policy course, and accelerate technological development accordingly.

The history of major cyber events points to the fact that the national security apparatus is multi-dimensional in the age of cyber. This implies that national security in the contemporary times is not limited to military capabilities. Generally, the defining features of a state's power include its capabilities to fight war, its institutions, and its ability to amend the norms of behaviour in the international arena. Therefore, the national security planners must work to protect the above three variables. These processes include the core security and conventional military procedures, systems that control the social and economic fabric of the country, political and institutional levels, and domestic political process. The domestic political process must be flexible to adjust to the prevailing expectations, especially in democratic states. The following section discusses these imperatives in detail.

## CONVENTIONAL SYSTEM

The military constitutes the basic element of national security and the most obvious cyber attacks include attacks on computer networks, exploitation and other defence techniques meant to safeguard the military capacity. Military forces can undertake numerous operations like disrupting enemy systems, enhancing the function of kinetic forces, or leverage exploitation techniques to gain an edge.

The issue for the military is not the new possibilities of technical attacks but the way they are deployed. The cyber conflict in the military is not limited to securing the state from foreign cyber attacks, nor does its sole focus lie in incorporating disruptive techniques into the military systems. The military is equally concerned about deploying digital techniques for intelligence, surveillance, and reconnaissance purposes along with coordinating with non-military bodies that are stakeholders in the national security apparatus. In addition, it also ensures that there is an unhindered flow of technological innovation, and all sorts of malicious meddling is forestalled. Furthermore, the military constantly needs to upgrade its doctrine for rules and regulations of engagement based on the needs of the digital age.

At this moment, adoption of a specific joint forces structure with jurisdiction over the cyber domain appears to be the norm for the creation of a centralised authority on network warfare as a coordinating structure for the armed forces across countries. For the US, it was the Joint Functional Component Command for Network Warfare which in its current form is called the US Cyber Command. This has allowed all other countries in Asia, Europe and Latin America to identify cyber space as a distinct domain, discrete from the traditionally operating domains of land, water, air, and space. A broad and incorporative purview of the Cyber Command would allow it to support, and share the responsibility of, other combatant commands in the hour of need.

However, a perennial issue that the forces around the world face is about developing an appropriate set of rules meant for interactions and engagements with the security actors of other states. Generally, military organisations are expected to align with the engagement rules of armed conflict outlined by states but the nature of cyber is different. It is not explicitly violent but is aggressive and has the capacity to disrupt the law and order situation of a foreign state, firms and civil society, as has been highlighted in the case of the cyber attack on Estonia. Hence, much like conventional warfare, the forces must specify the conditions in which a cyber attack is permissible, the specific profile for targets, along with the duration of the attack, and the lines of communication within the state that permit all forms of actions taken during the operation.

While the initial criterion is often maintained, and is relatively easy to induct, the aspect of lawfulness becomes challenging. This is due to the virtually non-existent threshold in the case of cyber: the barriers are often not easily regulated in a digital attack. Moreover, the quick action required in the cyber world often rules out the possibility of going by rank and file. The military-to-military or military-to-non-state actor interaction is a variable that depends on the procedure that the other country is following. This kind of decision-making where strategic central planning or debates are absent, is called the cybernetic model. In this kind of decision-making, it is the contestation of procedures that principally determines the contours of conflict incidents.[4]

The US uses the nomenclature 'Response Actions' (RAs) for defining the context of the defensive operation procedure.[5] The RAs have also laid down guidelines that describe the intensity and the events that require a response. They have marked out the kind of systems that should be attacked, for instance, they have ruled out zombie computers from the scope of attacks as they are not the real attackers. The main problem that comes in the way of the RAs guidelines is in the context of geography. In the case of conventional military operations, the range of retaliation from kinetic assets is predetermined and limited, and filled with layers of strategic security issues. Therefore, there is a strict demarcation and limit on the response boundaries. In cyber space, these conditions do not exist. The RAs must then be put in a context where the borders are 'technically' absent and the entire understanding around foreign threats has shifted.[6]

Another set of challenges for military establishments in terms of cyber space is weapon development and talent acquisition. Both these cases advance with the threat actor. Cyber is unique in the manner that with each attack, the possibilities and understanding of the state actor grow. The

[4] Alex Mintz, *Understanding Foreign Policy Decision-Making* (Cambridge: Cambridge University Press, 2010).

[5] National Research Council, *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009). Accessed on March 5, 2023.

[6] Ibid.

**In addition, cyber relies on the talent and brains of the hackers and how best they exploit the resources.**

need for adaptation works as an impetus for constant and quick modification. Moreover, it also depends on the technological innovation and electronic upgradation that take place, unlike earlier when military assets and their upgradation comprised an isolated affair. Both the national and global technology infrastructure innovation becomes a factor that must be taken into consideration while planning.

In addition, cyber relies on the talent and brains of the hackers and how best they exploit the resources. For this, talent acquisition becomes an important aspect.[7] The military requires to retain people with the ability to help with the cyber infrastructure in the wake of a global marketplace that lures and traps such special talents. Either the military works its way to bridge the gap and allows individuals from the private sector to step in, or entices them with a position that makes them stay.[8]

## CRITICAL INFRASTRUCTURE

The advent of cyber has brought with it the issue of critical infrastructure. Following the Oklahoma City bombings in 1995, a series of commission reports in the US mentioned the term "Critical Infrastructure" and has come to define various sectors of the nation that are crucial in the sense that any attack on one will have a direct impact on welfare and national security.[9] This includes a wide variety of sectors, from agriculture to water systems, railway networks to nuclear energy.

In the case of cyber, the attack on the Trans-Siberian pipeline is said to have started the debate that brings cyber and critical infrastructure in the same line. With the advances in technology, this threat has only multiplied manifold.

[7] Martin C. Libicki, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (Santa Monica, CA: RAND Corporation, 2014). Accessed on March 5, 2023.

[8] Ibid.

[9] Robert T. Marsh, "Critical Foundations: Protecting America's Infrastructures" (Washington, DC: The President's Commission on Critical Infrastructure Protection, 1997). Accessed on March 5, 2023.

Jeffrey Hunker has given the concept of tightly or loosely coupled sysytems to explain the reliance of this critical infrastructure on information systems.[10] Tightly coupled systems are the ones where disruption in one sector affects the other parts as well. Whereas, in a loosely coupled system, the effects are slow. For instance, while agriculture is an important sector and an attack on it will cause trouble, the intensity would be low. On the contrary, tightly coupled sectors like energy, banking and transportation will have serious impacts. The most important of these remains telecommunications because it governs the ability of the other sectors, and is crucial while mapping cyber conflict situations.[11]

**While agriculture is an important sector and an attack on it will cause trouble, the intensity would be low. On the contrary, tightly coupled sectors like energy, banking and transportation will have serious impacts.**

While states are always seeking to secure these infrastructures, difficulties arise when the policy that is floated has to be in coordination with the other sections of the national economies, especially in the case of democratic countries. For instance, a kill switch system would authorise an individual or selected group to shut down the internet of the entire country through the control of ISPs but this option would not go well with the stakeholders from the industrial and business groups. Hence, this brings the state into direct contestation with the private sectors, which raises the issue of bringing the two on the same plane.

## KNOWLEDGE IS POWER

The innovation industry directly determines the operational capacity of major national security elements, particularly in the context of cyber. This view has been echoed in the understanding of numerous International Relations (IR) scholars, where the technical lead in the long term translates

[10] Peter M. Shane, *Cybersecurity: Shared Risks, Shared Responsibilities* (Carolina Academic Press, 2013). Accessed on March 5, 2023.

[11] Ibid.

into the state's power potential, largely because this innovation is linked with economic growth and development. Therefore, digital intrusion on a large scale and data theft from private companies and government agencies account for a systematic change in the power dynamics of the states.[12] Albeit, the state that steals still faces difficulties in absorbing the information and its application but it adds to its short-term benefits.[13] An estimate of the annual intellectual property theft gave a figure that ranges somewhere between $2 billion to $400 billion. These numbers may not be alarming when compared to the global Gross Domestic Product (GDP) that runs in trillions, but points at the potential of exploitation.

The most obvious outcome of these thefts is the direct transfer of sensitive intelligence and technology from the government defence zone to the infiltrators. Some reports claim that in 1025, China stole nearly 50TB (Text Book) of information from the US government that included blueprints for weapons like the F-35 Lightning II fighter craft. Likewise, cyber attacks in the past like Titan Rain, Moonlight Maze, Shady Rats were also linked to the theft of unclassified and classified documents.[14] Such thefts weaken the position of the state by exposing their vulnerabilities to the attacker.[15]

Apart from putting the defence forces of a state at a disadvantage, intellectual theft also affects the private sector involved in technological innovation. It brings down the incentives of startups and many of them suffer from the loss of the first mover advantage. It further discourages private industries from collaborating with the government.

[12] Christopher Whyte, "Developed States' Vulnerability to Economic Disruption Online," *Orbis* vol. 60, no. 3, 2016. Accessed on March 5, 2023.

[13] Christopher Whyte, "Power and Predation in Cyberspace," *Strategic Studies Quarterly*, vol. 9, no. 1, 2015. Accessed on March 5, 2023.

[14] Siobhan Gorman and August Cole, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal 21*, April 21, 2009, www.wsj.com/articles/ SB124027491029837401. Accessed on March 5, 2023.

[15] James A. Lewis, "Computer Espionage, Titan Rain and China," Centre for Strategic and International Studies, Technology and Public Policy Programme (2005). Accessed on March 5, 2023.

## THE STATE STRUCTURE

Technology also modifies the information environment in which international affairs take place. The ways individuals and society share information have changed and with this the understanding of complex issues related to national security has also been modified. Information is subject to greater manipulation and involves a range of actors.

The way the economy directly impacts a nation's potential, the available information and discourse in a country also shapes the state's approach to foreign engagements and policies. The structure of the state is of significant concern here. The initially elaborated incident of cyber history had a common thread: a majority of threat actors that were identified were from non-democratic states like China, Russia, North Korea, and, most of the time, running on a proxy. The authoritarian state structure allows them to mould the policies as per their fancy. However, this is not the case for democratic and responsible regimes. In these countries, the government comes into being following a political process that includes a social discourse and interaction. This social interaction is an ideational marketplace for democracies. As information flows through, individuals change their preferences and tilt towards what they believe is the best suited option. Hence, the person in charge of taking decisions cannot work outside this model and this, in turn, incentivises non-democratic states to meddle in their affairs. Often, they try to interfere in the democratic processes of these units, flood the social platforms with manipulated information and engage in rhetoric that suits their agenda.

## CYBER CENSORSHIP

A relatively underexplored aspect of cyber war has been cyber censorship. The attack on Sony Pictures Entertainment and their halting the release of the movie due to foreign intervention is an issue states would require to deal with at length. While not all states allow the same level of freedom and rights to their citizens, the intention is to protect the ethos of their country.

**The speculation that goes around cyber war is that it is always huge scale attacks which destabilise the system, as was the case with Stuxnet.**

As the cyber attacks become more rampant, this aspect of freedom would be at the mercy of the attackers. The fact that it does not stop at things like movies, and can become an effective blackmailing tool is a cause of worry. It compromises the freedom of an individual, and also puts his life at risk because then he is constantly being monitored. This breaches all the fundamental rights, from privacy to expression. Therefore, states need to evolve a mechanism to safeguard crucial aspects, monitor social media platforms, and protect national telecasting agencies from such risks.

These factors clubbed together bring us to the possibility of a cyber war and whether it is likely to take place. The chances of a war entirely in the digital domain are bleak since a majority of experts believe that cyber conflict in isolation does not improve national war-fighting capabilities. Historically, cyber events have majorly brought out their role as force multipliers.

At best, three scenarios of cyber conflict have been expected and studied by scholars based on the range of cyber incidents in the past. The first one is where the disruption to the states is minimum because it focusses solely on the military systems. The speculation that goes around cyber war is that it is always huge scale attacks which destabilise the system, as was the case with Stuxnet.

The other two cyber scenarios consider more realistic grounds. In some cases, it takes the form of an effective cyber blockade.[16] This blockade includes a denial of service against the internet of the whole nation. This was achieved by a Russian hacker group in Estonia and in Georgia. North Korea also met a similar fate at the hands of the US in the Sony Pictures Entertainment case.

Lastly, a cyber war may become a broad scope attack when it targets the critical infrastructure of the country. This is the scenario that most

[16] Alison Lawlor Russell, *Cyber Blockades* (Washington, DC: Georgetown University Press, 2014). Accessed on March 5, 2023.

security experts are worried about. The attack on infrastructure has a domino affect on all the linked sectors in one way or the other.[17]

**In the absence of additional tools of violence and safeguards, cyber capabilities alone are not guarantors of long-lasting massive victories where states end up annexing territories, or change the status quo of a country.**

These cyber attacks can be used by states for multiple reasons. They might want to use them as a threat of violence and escalate them into the domain of coercion. This leads to the situation of compellence where states are forced to change their behaviour due to the threat of force. This contrasts with the policy of deterrence where attempts are made to avert an action by the state that otherwise it would have taken. While in conventional military setups, these mechanisms are explicit, in terms of cyber, they have an embedded complexity. Nevertheless, the prevalent nature of cyber has been more aggressive and less violent.[18] For instance, it reaches extremes in cases like Stuxnet which is a rare event. In the majority of cases, the havoc wreaked by cyber is temporary and the offensive front is moderated. This simply translates into the fact that in the absence of additional tools of violence and safeguards, cyber capabilities alone are not guarantors of long-lasting massive victories where states end up annexing territories, or change the status quo of a country. Hence, this puts cyber in a category where it is seen more as an adjunct modifier of war where it relies on various other elements of the security architecture like conventional military weapons, intelligence, and diplomatic channels to achieve some substantive foreign policy outcome.[19] But this limited understanding of cyber has been coming to an end with the increased dependence of states on technology and the innovations in the digital age. As these offensive actors embark on their journey of destruction,

[17] Brandon Valeriano, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford University Press, 2018). Accessed on March 5, 2023.

[18] Gartzke, n. 3.

[19] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, vol. 35, 2012. Accessed on March 5, 2023.

they would seek to penetrate the control and command of the nuclear facility, energy grid, etc where the damage will be irreversible.

## THE DIGITAL SECURITY DILEMMA

The aforementioned points bring us to an important question about the possibility of states relying entirely on cyber weapons. This can be answered by analysing the digital security dilemma that exists amongst the states.[20]

The security dilemma or the spiral model refers to a situation where an effort by a state to strengthen and mobilise its ability triggers other states to make an attempt to mobilise their resources as a response. This happens primarily for two reasons: first, because states have no mechanism in place to gauge the intention of the other, so, even if a state is increasing its ability without any hawkish reasons, it is never read that way; second, in the absence of a global government regime and police force, a state is constantly vulnerable to attack from another state. Hence, it must keep up with its peers to maintain the balance of power. This security dilemma is calculated through factors like whether the military technology inducted is offensive or defensive along with the perception that the states involved have about the utility of that technology.

When it comes to cyber, determining whether it is offensive or defensive is difficult. To answer this, we need to understand the attribution problem.[21] The problem arises because it is difficult for experts to identify attackers in the case of a cyber incident. This is true on almost all fronts. Firstly, the cyber apparatus in the case of a major cyber war allows the attacker to elude detection. Detection has been an issue in cyber for long. Moreover, not all cyber attacks happen as planned.[22] In some cases, due to insufficient information about the intended target's computer system, the desired goal

[20] Robert Jervis, "Cooperation under the Security Dilemma," *World Politics*, vol. 30, 1978. Accessed on March 6, 2023.

[21] Erik Gartzke, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies*, vol. 24, 2015. Accessed on March 6, 2023.

[22] Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution", *Journal of Conflict and Security Law*, vol. 17, 2012. Accessed on March 6, 2023.

may not be achieved. This makes it difficult to detect because the detection is designed around a specific type of attack.

In case the attacker is detected, the path of full attribution is not smooth. Technical information that allows the defender to access the entire information, from the nature to the source and place of the attack, is difficult to get. Especially when the intrusion is well planned and executed. As in the case of Moonlight Maze: it happened within minutes and this left a short window for the defenders to investigate and draw inferences. This does not imply that attribution is impossible, but the process becomes complex and takes time because to have the full story requires specialised equipment and resources along with cooperation with dozens of agencies.

Lastly, even when the technical attribution is identified, there still lies a difficulty in assessing responsibility. For instance, even after identifying the location of the Internet Protocol (IP) address, it can very well be the case that the operation took place from a 'zombie computer' or one that belongs to a non-state hacker. Therefore, to put responsibility on the state government becomes next to impossible.[23] This problem benefits the offender, hence, demarcating the offensive-defensive boundary in cyber becomes complex.[24]

The attribution problem at the defender's end helps to deceive attackers. For instance, in the case of Moonlight Maze or Cuckoo's Egg, the technique deployed by the defenders was Honeypot to entrap the intruders. They indeed manage to nullify the expected objectives and gains from the operation. In addition, the attackers generally refrain from regular intrusion as it gives the defender warning and opportunity to disrupt the expected attack. Moreover, a cyber attack is more of a forced interaction. At times, the defender finds it desirable to intrude as this gives him access and knowledge about new network vulnerabilities and back-hack incentives where the defender can disrupt or infect the attackers.[25] So, instead of passing cyber as an offensive

[23] Thomas and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, vol. 38, 2015. Accessed on March 6, 2023.

[24] Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack", *Journal of Cybersecurity*, vol. 1, 2015.

[25] Gartzke, n. 21.

dominant discourse, it would be more accurate to call it an 'offence enabling' domain. Technology facilitates the attackers but that does not mean it leaves the defender *defenceless.* Provided good capital expenditure and effective designs, systems can be secured in a way to deter an attack.

The next aspect of the security dilemma is about perception. Analysing perception is a difficult task because it entails predicting psychological factors. This becomes more difficult in the case of cyber because of the complex decision-making system involved where decisions are taken at the level of the executive while operational behaviour varies across the units of the security architecture. Moreover, it is not easy to quantify perception, and intention analysis is another challenge that the governments face.

## THREAT TO MILITARY FACILITIES

Cyber attacks can significantly harm the Command and Control (C2) of military facilities by targeting their communication systems, computer networks, and information infrastructure. These attacks can exploit vulnerabilities and weaknesses in the C2 systems, compromising the ability of military commanders to effectively lead, coordinate operations, and make critical decisions. Given below is an in-depth exploration of how cyber attacks can harm the C2 of military facilities, along with some examples:

- **Communication Disruption**: Cyber attackers can target the communication systems used by military facilities to relay commands, exchange information, and maintain situational awareness. By disrupting these systems, adversaries can sever the lines of communication between commanders and their subordinate units, causing confusion, delays, and a breakdown in coordination. For example, in 2008, the US military experienced a cyber attack known as Operation Buckshot Yankee, where a malware infection disrupted the network used by the Central Command, impacting its ability to communicate and share information effectively.
- **Manipulation of Command Information**: Cyber attackers can manipulate or alter the information flowing through the C2 systems, leading to inaccurate situational awareness and compromised decision-making.

By tampering with data such as intelligence reports, sensor readings, or mission orders, adversaries can mislead military commanders and influence their judgment. For instance, in 2015, the Russian military allegedly conducted a cyber attack against Ukraine, compromising the command information systems and providing false orders to Ukrainian artillery units. This led to misdirected fire, enabling Russian-backed forces to gain a tactical advantage.

- **Targeting C2 Infrastructure**: Military facilities rely heavily on computer networks, servers, and other infrastructure to support their C2 operations. Cyber attacks can target these critical components, disrupting or disabling them entirely. For example, in 2007, the Estonian government and military institutions faced a series of cyber attacks that targeted their C2 infrastructure, leading to the disruption of governmental websites, email systems, and other critical services. These attacks caused significant challenges in coordinating and responding to the situation.
- **Command Deception**: Adversaries can use cyber attacks to deceive military commanders by manipulating or falsifying information related to enemy positions, intentions, or capabilities. By feeding false intelligence, attackers can influence the decision-making process and cause commanders to make suboptimal choices. This type of deception can lead to mission failures, increased casualties, or strategic setbacks. For instance, during the Gulf War in 1991, the US military launched Operation Desert Storm, where it conducted cyber attacks against Iraqi radar systems. By manipulating the radar data, it deceived the Iraqi military, leading it to believe that the US forces would attack from a different direction than the actual plan.
- **Targeting Commanders' Personal Devices**: Military commanders often rely on personal devices, such as smartphones or tablets, to access sensitive information or communicate with their staff. Cyber attackers can compromise these devices, gaining unauthorised access to confidential data, personal communications, or even eavesdropping on voice conversations. By infiltrating the personal devices of military leaders,

adversaries can gather valuable intelligence, compromise operational security, or potentially blackmail and coerce decision-makers. Although specific examples in this regard may not be publicly available, the potential risks of such attacks on personal devices are significant given the prominence of mobile technology in modern military operations.

- **Insider Threats and Social Engineering**: Cyber attacks on military facilities can also exploit insider threats or employ social engineering techniques to gain unauthorised access to C2 systems. Insider threats may involve compromised personnel or individuals coerced into providing access or sensitive information to adversaries. Social engineering tactics, such as phishing emails or impersonation, can deceive military personnel into revealing login credentials or executing malicious actions. These tactics can enable attackers to infiltrate the C2 systems, potentially compromising the confidentiality, integrity, and availability of critical information.

These attacks have the potential to undermine the effectiveness of military operations, compromise operational security, and cause strategic setbacks. It is crucial for military organisations to prioritise cyber security measures, implement robust defences, conduct regular training and awareness programmes, and continually adapt to emerging cyber threats to ensure the resilience of their command and control.

## CONCLUSION

The history of cyber is also a history of how state capabilities have developed to counter new ranges of threats that surfaced and this, in turn, has modified the state security architecture. Cyber has been multifaceted in its approach because it has bypassed the conventional security norms where militaries would interact. It has now entered the domain of non-traditional security and there is no specific design in which cyber can operate. It can either attack the critical infrastructure or it can act as a force multiplier. Though it has played a limited role as a violent actor, that potential remains intact.

The complexities inherent in the cyber domain make it difficult for security experts to employ traditional war mechanisms and understanding to deal with it. For instance, in the case of a security dilemma analysis, it cannot be put in just one domain of offensive or defensive. There is always a grey area in which it operates. A problem that has been recurring in cyber conflict is to bring the hackers to terms. Generally, it is the zombie computers or the states using a proxy front. Hence, even if the culprit is revealed, it does not translate into an actionable justice process. That end is always left loose, and to tighten it up, a robust law mechanism needs to be in place. However, when it comes to cyber laws, a whole new dimension opens up because the states involved in the law-making process are not willing to close these loose ends as this absence of order helps their hawkish intentions. Hence, a lot transpires in the domain of cyber which cannot be equated to the conventional way of dealing with security that states are used to. States need to reformulate and reconfigure their security dynamics around these new lines where they can tap into new possibilities, and in this venture, they should understand the involvement of multiple stakeholders. So far, the private sector has been not fully inducted in the state technological apparatus which is affecting the states' capabilities.