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

CCG NLU, DELHI *on* AUGUST 8, 2020

8 MINUTE READ

By Gunjan Chawla and Vagisha Srivastava

In our previous post, "Does India have offensive cyber capabilities?", we discussed a recent amendment to the SCOMET list appended to the ITC-HS classification by the Directorate General of Foreign Trade (DGFT). The amendment did not define, but described software for military offensive cyber operations as a term including (but not limited to) software which are designed to destroy, damage, degrade or disrupt systems, equipment and other softwares specified by Category 6 (Munitions), as well as software for cyber reconnaissance and cyber command and control.

In this post, we examine what exactly constitutes 'offensive cyber capabilities' (OCCs) and their role in conducting cyber operations with reference to various concepts from US, UK and Australia's cyber doctrines. We begin by comparing two definitions of 'cyber capabilities'.

'Cyber Capabilities' = 'Cyber Operations'?

In US military doctrine, a 'cyberspace capability' is defined not as human skill in handling tools and software, but as "**a device or computer program**, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace." (emphasis added)

In contrast, the Australian Strategic Policy Institute (ASPI) in Defining Offensive Cyber Capabilities notes that "In the context of cyber operations, having a capability means possessing **the resources, skills, knowledge, operational concepts and procedures** to be able to have an effect in cyberspace." [emphasis added]

The ASPI's emphasis on resources, skills and knowledge merits special attention. Without skilled personnel to wield such devices or software, offensive cyber operations cannot be mounted successfully. This is an especially important distinction if we are looking to formulate a functional definition relevant to India's requirements. Our conceptualisation of OCCs must accord priority to not only the

acquisition of tools, devices and software developed by other nations, but to build internal capacity through investment in creation and dissemination of technical knowledge and skill development.

This view also finds support in the United Kingdom's articulation of defence 'cyber capabilitiy'. In the UK's Cyber Primer formulated by the Ministry of Defence, it is acknowledged (see fn 7) that defence cyber capabilities can be **a combination** of hardware, firmware, software and operator action (emphasis added).

Yet, surprisingly, the ASPI's concluding definition of OCCs equates *offensive* capabilities with offensive cyber operations (OCOs), "offensive cyber **capabilities are defined as operations in cyberspace** to manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks." (emphasis added)

The underlying logic of this equation is perhaps the old adage — the proof of the pudding is in the eating? This means that in ASPI's conceptualisation, to 'have' OCCs would be meaningless, and not entirely credible if no OCOs are conducted by entities claiming to possess OCCs. However, from a legal standpoint, one cannot say that 'capabilities' and 'operations' are synonymous any more than one could claim that having 'arms/ammunitions/weapons' are synonymous to an 'armed attack'.

This leads us to an obvious question — what are offensive cyber operations?

Offensive Cyber Operations: Cyber Attacks (or Exploits) by Another Name?

In the United States' military doctrine, Offensive Cyber Operations (OCOs) are understood to be operations that are "intended to project power by application of force in or through cyberspace."

This definition of OCOs is also reiterated in the March 2020 report of the Cyberspace Solarium Commission (CSC). The CSC was constituted last year by the US Congress under the John S. McCain National Defense Authorization Act, 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences" and presented its report to the public on 11 March 2020.

Over the years, the vocabulary of the US military doctrine and strategy documents of the Department of Defense (DoD) too, have used a variety of terms to classify various categories of cyber operations. In 2006, the DoD preferred using the broader term 'Computer Network Operations' (CNOs) instead of 'cyber attacks', as seen in its National Military Strategy for Cyberspace Operations. CNOs were classified into computer network attack (CNAs), computer network defense (CND) and computer network exploitation (CNEs).

More recent documents have dropped the use of the term 'CNO' and exhibit a preference for 'cyberspace operations' or 'cyber operations' instead. The US DoD *Dictionary of Military and Associated Terms* defines 'cyberspace operations' as '[t]he employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace'.

Yet, in spite of the multiplicity of terms employed, offensive cyber capabilities can be categorised broadly as the ability to conduct a cyber attack or cyber exploitation. Although similar, it is important to distinguish cyber attacks from cyber exploitations. Herbert Lin has observed that "[t]he primary technical difference between cyber attack and cyber exploitation is in the nature of the payload to be executed—a cyber attack payload is destructive whereas a cyber exploitation payload acquires information nondestructively".

Indeed, the US DoD dictionary defines 'cyberspace attacks' and 'cyberspace exploits' separately. 'Cyberspace attacks' are actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fire. In contrast, cyberspace exploitation refers to

actions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations'.

A definition of OCOs similar to the US' conceptualisation can also be found in the UK Cyber Primer. This Primer defines OCOs as "activities that project power to achieve military objectives in, or through, cyberspace".

The UK envisions OCOs as one of four non-discrete categories within the broader term 'cyber operations' that can be used to inflict temporary or permanent effects that reduce an adversary's confidence in networks or capabilities. Such action can support deterrence by communicating intent or threats. These four categories are, namely, (1) defensive cyber operations; (2) offensive cyber operations; (3) cyber intelligence, surveillance and reconnaissance; and (4) cyber operational preparation of the environment.

Thus, we can infer from a combined reading of all these definitions that

1. cyber capabilities and cyber operations are not synonymous, but
2. cyber capabilities (both the technological tools, as well as the human skill elements) are a prerequisite to conducting OCOs, which may be intended to either –
    - 'project power through the application of force' (US) or
    - 'achieve military objectives' (UK) or
    - 'manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks' (ASPI) or
    - 'destroy, damage, degrade or disrupt systems, equipment and other softwares (India's DGFT) – in or through cyberspace.

A one trick pony?

In order to execute an offensive cyber operation, the tools (or capabilities) used could range from simple malware, virus, phishing attacks, ransomware, denial of

service attacks, to more sophisticated and specially-built softwares. But these tools would be futile if not for the existence of vulnerabilities in the system being attacked to enable the exploit.

From the standpoint of conducting an offensive cyber operation (whether an attack or exploit), one would necessarily require:

1. Cyber capabilities (technical tools and software) to exploit a pre-existing vulnerability, or to introduce a new vulnerability into the targeted system
2. A specific intent (i.e. specific orders or directions to meet a particular, specified military or strategic objective through on in cyberspace)
3. A person/organization/entity/State identified as the target and (i.e. an intended target)
4. Planning and clearly defining the expected consequences of the attack (i.e. the intended effects)

The presence or absence of any of these factors would heavily determine the likelihood of the success of a cyber attack or exploit. Often, the actual outcome of a cyber attack is different from the intended outcome. As one cyber intelligence analyst puts it, "Any cyber operator worth her salt knows that even mission-driven, militaristic hacking thrives under great, terrifying ambiguity."

Additionally, while the tools used are time-consuming to produce, they are rendered useless after deploying an attack. In most cases, this is because operators of the system being attacked will ensure the application of security patches to close known vulnerabilities in the aftermath of a cyber attack. For this reason, OCCs, especially those that have been 'specially designed or modified for use in military offensive cyber operations', once deployed, have extremely limited to negligible potential for re-use or re-deployment, especially against the same target. However, without sufficient emphasis on and investment in human skills and capabilities, the effectiveness of the available technical tools would also suffer in the long run.

A ‘digital strike’ to start a ‘cyber war’?

The deployment of cyber capabilities in an OCO must cause actual physical damage comparable in scale and effects to that of a conventional, kinetic attack to be termed as an ‘armed attack’ or an unlawful ‘use of force’ in international law. Although some of the attacks or exploitations in cyberspace could result in physical damage akin to damage caused by a traditional kinetic attack, most don’t.

Drawing from a list of significant cyber incidents recorded by the Center for Strategic and International Studies (CSIS), we can observe that very few attacks carried out in the past had the potential to lead to casualties. Scholars still disagree if all these cyber incidents could be termed as ‘a use of force’ or ‘a tool of coercion’ in international law.

However, it is interesting to note that the *intent* of the perpetrator of a cyber attack, a crucial element that is baked into American definitions of OCOs, is conspicuously missing from the international law analyses to classify cyber attacks as a ‘use of force’ or ‘armed attack’ – which relies largely on the scale and effects (actual, not intended) of the cyber attack. (see Tallinn Manual 2.0, Rules 69 and 71) The omission of any reference to human skill or judgment in the US’ definition of cyber capabilities too, provides additional insulation from inquiries into the actual intent of the perpetrator of a cyber attack.

At this point in time it is difficult to conceptualize a ‘war’ that is waged exclusively in cyberspace, does not manifest physical effects or spill over into other domains—not just air, land and sea, but also the economy. For this very reason, i.e. the interconnected nature of cyberspace with other domains of where conflict manifests from competing interests, OCCs provide States a strategic military advantage by strengthening the effectiveness of conventional means and methods of warfare and streamlining military communications. However, the increasing dependence of the Government, critical infrastructure as well as businesses on the internet in the networked economy necessarily implies that a failure to develop or

acquire cyber capabilities will make regular economic losses and disruptions by way of cyber attacks inevitable.

This leads us to another question worth considering in the context of State hostilities in cyberspace—whether economic losses occasioned by cyber attacks can be considered as a factor in determining whether its scale and effects are comparable to that of a kinetic armed attack?

Both cyber attack and cyber exploitations hold the potential to cause economic losses to the State under attack. Today it is common knowledge that the notorious WannaCry and NotPetya attacks resulted in losses totalling up to billions of dollars. Attacks on financial systems, commercial softwares, platforms or applications that generate economic value, or civilian infrastructure linked closely with the state economy could all fall under this risk. Such attacks can also substantially slow down State functions if the chaos generated within cyber systems spills over into the physical realm.

We must also remember, that any response to this question cuts both ways – if India – or any other nation – wishes to treat economic losses caused by hostile States and other actors in cyberspace as indicative of an unlawful 'use of force' or an 'armed attack' in cyberspace, we must also be prepared to have our adversaries draw similar conclusions regarding economic losses inflicted upon them, and anticipate retaliatory action.

Given the massive risks to the economy associated with a high incidence of cyber attacks, it would be interesting to observe what direction the debate on offensive cyber capabilities takes with the release of the National Cyber Security Strategy 2020. With India's cyber ecosystem under development, both the cyber offence and cyber defence capabilities are of immense strategic value and merit a deeper exploration and stricter scrutiny by policymakers.

This question lingers as an especially intriguing one, as the amendments to Appendix III of the ITC-HS classification referred to in our last post have now been taken down from the website of the Directorate General of Foreign Trade, only to

be replaced by a sanitized version of the SCOMET list amended on 11.06.2020 – one that includes no reference 'military offensive cyber operations' or even 'cyber' *simpliciter*. Even the reference to 'intrusion software' under head 8E401 has now been omitted. The version of the SCOMET list that we relied on for our previous post is no longer available on the DGFT website, but for interested researchers, can be downloaded here on CCG's Blog.

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

Support our journalism:

For You

DISCOVER MORE

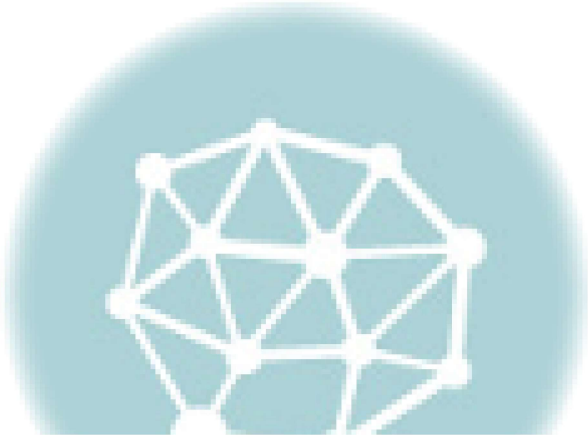
cyber security | cybersecurity | national cyber security strategy 2020

Related Posts:

Lt Gen. (Dr) Rajesh Pant on India's National Cyber Security Strategy, Indo-US cooperation, end-to-end encryption and more

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

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



Does India have offensive cyber capabilities? — by Gunjan Chawla

Airtel partners Symantec to distribute B2B cyber security solutions in India

Recommendations for improving cybersecurity governance in India

MEDIANAMA

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