India needs Cyber Weapons and Policy

– **Prashant Mali**
Cyber Warfare Researcher and Noted Cyber Lawyer, cyberlawconsulting@gmail.com

Cyber weapons are stealth weapons. They don't have the flash and bang of canons and missiles; they hit as in computer programs and are used to silently infiltrate individual machines and entire networks. They have the capacity to strike with great precision, shutting down critical infrastructure, confusing enemy signals, upending communications, and responding to and redirecting military attacks before they occur. Before India, ideally the question is no longer: "Should we do this?" The question is now: "Can we do this?

Introduction

As proposed by Trey Herr,"Cyber Weapons are any combination of three software components: a Propagation Method, one or several Exploits, and a Payload designed to create destructive physical or logical effects".The payload component is the mechanism that actually accomplishes what the weapons is supposed to do – destroy data, interrupt communications, exfiltrate information, causing computer-controlled centrifuges to speed up, and so on.If the payload causes data exfiltration, we call this cyber exploitation. If the payload causes damage, destruction, degradation, or denial, the use is called a cyber attack. Stratfor, for example, has described a "hair-trigger" world in which the most powerful cyber nations could unleash war using cyber weapons on each other with lightning speed and with no advance warning.

The use of a highly targetable cyber weapon may be as effective against a target as a kinetic weapon, but with significantly less risk of collateral damage.Cyber weapons that can be used in targeted cyberattackswhich cause excessive damage to unintended targets.This can be a catalyst for an undesired escalation of conflict, specially when we haveopprobriousneighbor's.

Just as cyber weapons themselves operate largely out of sight, so too the work of those combatants. Over

Reasons why India needs them?

1. Manufacturing of cyber weapons is much cheaper and faster than typical kinetic weapons. Once a cyber weapon has been reverse engineered and its mechanism of deployment and use recovered, making more of the same is far easier than the manufacture of other types of weapons. India hugely depends upon Russia and other countries for kinetic weapons. I believe there can be a time when Russia would supply us sensitive military hardware which is "Made in China"
2. Proliferation of cyber weapons is much easier than proliferation of kinetic weapons. Contrasting kinetic weapons that explode and destroy themselves as well as the target, a cyber weapon does not necessarily destroy itself upon use. Such a weapon, used to attack one target, is relatively easily recovered and some components may be reused.
3. Cyber warfare is a never-ending game of catch-up. In fact, this is an area where more spending doesn't guarantee better outcomes
4. Cyber weapons, will act as a counterbalance to other countries superiority in conventional and strategic weapons. International treaty if it ever happens, inspectors are unlikely to detect secret cyber weapons.
5. Usage of cyber weapons provides strategic deterrence as well.
6. India has large pool of civilian cyber security researchers or Ethical hackers, time and again they can be tested for loyalty and easily used as civilian volunteers with security clearances to find vulnerabilities and to build cyber weapons or respond to cyber attacks.
7. As the Internet is not yet balkanized, India stands a chance to establish cyber command and control mechanism of cyber weapons in the cyber space outside physical boundaries of India.
8. The U.N. charter and modern warfare conventions frown on preemption; nations can use force only for self-defense or when authorized by the Security Council. But cyber space violations have been tolerated neither the Bush nor Obama administrations consulted the U.N. before launching the Stuxnet virus to disrupt Iran's uranium processing facilities. Ukraine Power grid attack was an another example.

the years, despite publicizing the existence of this cyber strike force, and in the face of evidence culled from documents leaked by formerNSA contractor Edward Snowden that show that in 2011 alone the United States initiated 231 offensive cyber attacks, the government has never acknowledged launching a single one,

Now considering the dangerous of owning or using cyber weapons, I would like to thrust upon that attribution might also invite retribution, which indeed did happen when, beginning in 2011, the Iranians attacked forty-six American financial institutions over 176 days, including J.P. Morgan, the New York Stock Exchange, and Wells Fargo. In 2013 they hacked into the operating system of a New York dam. In June of 2019,Iranian cruise missiles and its command and control systems went down due to alleged US Cyber command attack. Attribution would also undermine the government's credibility when protesting the cyber incursions of other nations. So anonymity within the code and secrecy about it were crucial.

Nuclear weapons are expensive to build and maintain, and this is another way they are different from cyber weapons, which are cheap and available on the black market so that any country—and any criminal or terrorist group or proxy nation or industrial competitor—can acquire them. In 2014, for instance, hackers—their identity still unknown—infiltrated the control system of a German steel plant. The next year, hackers, most likely from Russia, shut down the power grid in western Ukraine. China, which has its own elite offensive cyber force within the People's Liberation Army, has been busy stealing, among many other things, blueprints for US pipelines, power transmission lines, and power plants.

Some five dozen countries are building a military-cyber operation, equivalent to the United States' Cyber Command.In the Department of Defense's lengthy report on its cyber strategy, issued in April 2015, the author notes that cyber threatshave displaced terrorism as the number-one strategic threat to the United States, and they name Russia, China, Iran, andNorth Korea as havinginvested significantly in cyber as it provides them with a viable, plausibly deniable capability totarget the US homeland and damage US interests.This could be true when seen towards India too.

That same document, most of which is devoted to cyber defense andCybersecurity, also acknowledges, in conditional and dissembling bureaucratic language, the Defense Department's willingness to engage in offensive cyber actions.

Conclusion:

Manycyber thinkersalthough have suggested that the existing rules that govern war are applicable to cyber conflicts as well, the stealth nature of cyber attacks, where attribution is often impossible to ascertain, holds the promise of absolving nations of the responsibility of adhering to them. The secrecy that enables one country to pick the pocket of another allows them to do so without international scrutiny. India with its large young population with analytical background, with many of them being patriotic, holds a better chance to develop policies around cyber warfare leading to cyber weapons equipped cyber command. For India cyber weapons may hold out the possibility of a certain kind of mutually assured destruction, but so far there has been little international interest in deterrence. I feel what India does today will decide its might in the current and future cyber space conflicts, hence the need for cyber weapons. We can empower NTRO or Military with permission for offensive operations but without budget for buying recent exploits or effective indigenous exploit hunting and bug bounty program supported by law would demotivate even the existing cyber warriors .

Advocate Prashant Mali is a Internationally renowned Cyber Law, Cyber Security & Privacy Expert, Author & a Practicing Bombay High Court Lawyer based out of Mumbai, India . He is also Founder & President of the award winning premier technology Law Firm "Cyber Law Consulting ". He has trained Police Officers & Judges in various Police academies including National Police Academy & National Judicial Academy. He had been awarded by the hands of Soli Sorabjee as "Best Cyber Lawyer 2017" by India legal summit n Awards. In 2016 was awarded as "Cyber Security Lawyer of the year-India by Financial Monthly magazine of U K and in past been awarded as "Cyber Security & Cyber Law Lawyer of The Year:2014" by Indian National Bar Association. He is Masters in Computer Science & Masters in Law with certification in Computer Forensics & Systems Audit with working experience in the field of IT Security & Law for more than 20 Yrs. He has been interviewed by amost all National TV Channels and Quoted by leading News papers of India & abroad .He regularly writes for leading magazines and is a passionate speaker at National & International Seminars.He has authored 8 books on Cyber Crimes & Cyber Laws. He is a legal adviser to Police, Govt Companies ,MNC's, Corporates and represents them in various courts. He has successfully argued and got decisions in landmark cyber cases as a legal counsel. He was invited by Oxford University to Present a paper on "Cyber Terrorism & International Law" and his abstract of Research paper namely " Defining Cyber Weapon A techno Legal perspective" was selected by NATO's Cyber Conflict Centre in Tallinn, Estonia and got published in IGI Journal. His PhD Research Interest is in Cyber warfare, Cyber Security, Cyber weapons and International Cyber Law. He is passionate speaker and invited in many National and International Conferences as key note on topics like Electronic evidence, Cyber Laws, Cyber Insurance,Social Media, Block chain, Data Privacy, ecommerce, Cyber security policy & IPR. He is a Noted Chevening(UK) Cyber Security Fellow and Participant of IVLP (USA) in "Linking Digital Policy to Cyber Crime Enforcement". His clients include Shapoorji Pallonji, World Gold Council, Deloitee, Asian Paints, Aditya Birla Group, Mastek, NSDL, UTI, Life Insurance Council, various Banks & Insurance Companies including celebrities like Sunny Leone, Ram Gopal Verma, Tiger Shroff to Name a few.

cyberlawconsulting@gmail.com