VIF PAPER | AUGUST 2021

CYBER WEAPONS
- A WEAPON OF WAR?

Maj Gen P K Mallick, VSM (Retd)

Vivekananda International Foundation

Published in 2021 by

Vivekananda International Foundation

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

Tel: 011-24121764 | Fax: 011-66173415

E-mail: info@vifindia.org

Website: www.vifindia.org

ISBN: 978-93-91498-00-9

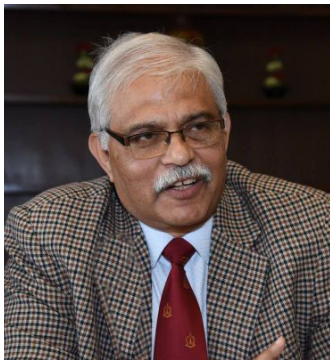
Follow us on

Twitter | @vifindia

Facebook | /vifindia

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 The author certifies that the article/paper is original in content, unpublished and it has not been submitted for publication/web upload elsewhere, and that the facts and figures quoted are duly referenced, as needed, and are believed to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

Cover Image Source : https://www.silicon.co.uk (Cyber war)



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

Cyber Weapons
- A Weapon of War?

Introduction

The character of warfare has changed fundamentally over the last decade. In the past, it was essential for an adversary nation or insurgent to physically bring weapons to bear during combat. That requirement is no longer a necessity. In cyber operations, the only weapons that need to be used are bits and bytes. In this new era of warfare, logistics issues that often restrict and limit conventional warfare and weaponry are not impediments. This new weaponry moves at the speed of light, is available to every human on the planet and can be as surgical as a scalpel or as devastating as a nuclear bomb.

Cyber attacks in various forms have become a global problem. Cyber weapons are low-cost, low-risk, highly effective and easily deployable globally. This new class of weapons is within reach of many countries, extremist or terrorist groups, non-state actors, and even individuals. Cyber crime organisations are developing cyber weapons effectively. The use of offensive Cyber operations by nation-states directly against another or by co-opting cyber criminals has blurred the line between spies and non-state malicious hackers. New entrants, both nation-states and non-state actors have unmatched espionage and surveillance capabilities with significant capabilities. They are often the forerunners for criminal financial gain,

destruction and disruption operations. Progressively, we see non-state actors including commercial entities, developing capabilities that were solely held by a handful of state actors.

The proliferation of cyber tools is lowering the barriers to entrance. The ability to buy capabilities off the shelf, bridge gaps in capabilities, or build tailored tools ensures the complex undercurrents of the current cyber threat landscape will remain to challenge national security, the commercial sector and civilians. The ability to buy cyber tools commercially permits state and non-state actors to leapfrog from emerging threats to established threats quickly. There are no clear redlines that set expectations and implications for using cyber weapons by state and non-state actors. This is a relatively new area of warfare, the rules of engagement are still emerging and unclear.

Among the most notorious private actors is the Russian Business Network, commonly known as RBN, which started as an Internet service provider for child pornography, phishing spam, and malware distribution. It has specialised in personal identity theft for resale. RBN provides scripts and executables to make cyber weapons undetectable by anti-virus software. Every time a cyber weapon is generated, it looks different to the anti-virus engines, and it goes through often undetected. The modularisation of the delivery platforms and malicious instruction is a growing design in cyber weapons. Cyber weapons of RBN are very popular and powerful.

Intelligence Community and militaries worldwide have developed new tools for exploiting, subverting, degrading and destroying adversaries' informational assets. This category of capabilities is loosely described as 'cyber weapons'. Cyber weapons are throwing serious challenges for public and private sector. Crucial issues include the dual-use nature of cyber weapons, attribution of cyber actions, use of cyber weapons as a force multiplier for traditional military operations and unpredictability and potential for collateral damage.

Offensive Cyber Operations (OCO) requires cyber weapons, people, planning, goals, command and control and rules of engagement. Cyber weapons provide offensive capabilities which can be used for offensive or defensive purposes. It has been noted by several scholars that "unlike

weapons of mass destruction, cyber weapons are an integral part of the commander's arsenal in conducting force-on-force and asymmetric warfare and will be used in concert with kinetic weapons to soften up the adversary's defences." Therefore at the operational/tactical level, there is a need to coordinate between offensive cyber operations and information operations/activities.

Definition

There is no single definition of Cyber Weapons. In 2011, the U.S. Department of Defense acknowledged that "the interconnected nature of cyber space poses significant challenges for applying some of the legal frameworks developed for specific physical domains" and that "there is currently no international consensus regarding the definition of a 'cyber weapon."[1]

The Dictionary of Military and Associated Terms of the U.S. Department of Defense defined cyber weapons as "a weapon that is explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment."[2] The *Tallinn Manual* characterises cyber weapons by their effects, not by how they are constructed or their means of operation. It is defined as, cyber weapons are cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack. Rid and McBurney define cyber weapons as «computer code that is used, or designed to be used, to threaten or cause physical, functional, or mental harm to structures, systems, or living beings. This definition respects the established understanding of a weapon as «an offensive capability that is applied, or that is intended or designed to be applied, to an adversary to cause death, injury or damage.

A cyber weapon is a software-based IT tool that can affect damaging, destructive or degrading effects on the network system against which it is directed. Cyber weapons can be installed in hardware as well. Backdoors can be embedded in hardware and installed at any point in the supply

chain, from initial fabrication as commodity hardware to the process of shipping a finished system to an end-user. 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.

To reach a definition of cyber weapon, it is necessary to focus on three essential elements:-

- **The Context**. This may be defined as a conflict among actors, both national and non-national, characterised by the use of technological information systems, to achieve, keep or defending a condition of strategic, operative and/or tactical advantage.

- **The Purpose**. Causing physical damage to equipment or people or sabotaging or damaging the information systems of a sensitive target of the attacked subject in a direct way.

- **The Means/Tool.** An attack through the use of technological information systems, including the Internet.

An analysis of the present weapons shows that cyber weapons:- [3]

- Can combine action at a distance, with close-quarters accuracy and efficiency, permitting a new class of attacks that are de-risked versus conventional means.

- Arrange for the capability to strike rapidly, without warning across an entire network, propagating faster than investigators can react.

- Have reversible effects and are limited in duration, allowing attacks to be used for signalling, to disrupt but not destroy infrastructure.

- Are most effective when they augment kinetic capabilities offering a new, wider-reaching and crucially deniable means of carrying out these activities.

- Provide the ability to reach out and conduct influence operations faster and cheaper than would otherwise be possible to do without cyber space.

Elements of Cyber Weapons

Typical elements of a cyber weapon are:-

- The aim must be specific.
- The information systems to be hit must be classified as a sensitive target.
- The purpose should be to actively penetrate the target's information systems with malicious ends.
- The information systems of the initiator must be protected.
- Tangible or significantly detectable damage must be caused.

The cyber weapon is the combination of three factors:-

- **Vulnerability**. Vulnerabilities are properties inherent in the systems (hardware or software) that one seeks to hack. Weakness or flaw in hardware or software that can be taken advantage of by an attacker.
- **Exploitation**. Programs are written to take advantage of a vulnerability and cause a specific effect, such as gaining access to a system or shutting down a piece of hardware.
- **Propagation Method**. In this, an exploit is delivered to a target, such as through a phishing email.

Cyber weapons are written in computer code. They can infiltrate whole networks or infect individual computers. They rely on software vulnerabilities, poor cyber hygiene and people who inadvertently open attachments infected with malware. They can confuse the enemy, and shut down military attacks before they occur and baffle communication systems. According to Eric Rosenbach, the Pentagon's cyber czar during the Obama Administration, offensive cyber activity is a "painstaking work" that involves identifying a platform in another country, gaining access,

and then remaining undetected, often for years, inside the system. A lot of hard work is done beforehand to figure out what targets to hit and maintain access to them.

Cyber attacks often create cascade effects that were outside the original intentions of the attacker. Analysis of malicious code used in latest sophisticated cyber attacks and reverse-engineering have revealed four common characteristics that help provide a more precise and practical definition for a cyber weapon:- [4]

- A stealth capability that allows undetected operation within the targeted system over an extended time period.
- A campaign that can combine various malicious programs for espionage, data theft or sabotage.
- An attacker with detailed knowledge of the workings of the targeted system.
- A special type of computer code to evade protective cyber security technology.

The question of using cyber weapons is contentious. When nation-states and other actors start to increase offensive cyber capabilities, there is always the possibility of escalation. Unexpected side effects may occur when releasing cyber weapons. Strategic uses of cyber weapons focus on longer-term, more overarching goals and are designed to affect the broader dynamics between potential adversaries both on and off the hot battlefield. Tactical uses of a cyber weapon focus on short-term, narrow goals — how to defeat the adversary in the next obstacle tomorrow. There is a need to coordinate between offensive cyber operations and information operations/activities at the operational level.

Components

A cyber weapon has two components: a penetration component and a payload component.

The Penetration Component. It is the mechanism through which the weapon gains access to the system to be attacked. Penetrations can occur using well-known vulnerabilities, including those for which patches have been released. The majority of attacks are accomplished in this way. Some use 'zero-day' vulnerabilities, which are vulnerabilities that are discovered and exploited before being disclosed to the vendor or otherwise being publicly disclosed. This can be accomplished by remote access, like sending an email with an infected attachment, by connecting to the target's wi-fi router or by compromising websites. It can be done by wireless code insertion transmitted over radio or radar frequencies. It can also be done by direct access, forming a direct connection to the target system through a USB drives.[5] Some pieces of malware like Stuxnet use more than one propagation method to get to the target system.[6]

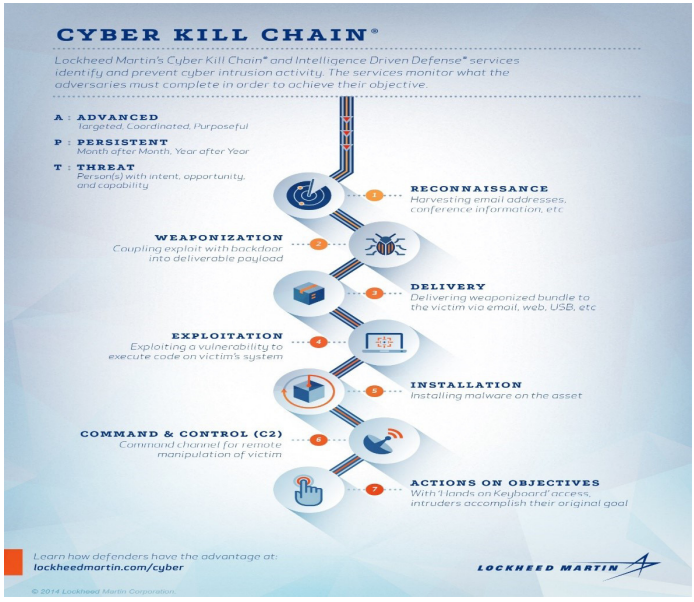
Counterfeit hardware, software and electronic components can be used as delivery vehicles. It permits the malicious payload to reach a specific target inside a computer, system or network. Vulnerabilities in software and computer system configurations offer entry to the payload. These security exposures allow for exploitation and compromise. It helps unauthorised remote access and control over the system.

Propagation methods are regularly adjusted to the nature of the target and the identified vulnerability. In the case of the SolarWinds supply-chain attack, the attackers got access to the source code of a popular network management system; via the software vendor's update servers the infected software was distributed to the target.[7] In the Stuxnet incidnce, the attackers first infected the private computer of a Natanz nuclear facility employee through phishing emails. They then made sure that the malware was carried onto the target system by the unsuspecting employee on a USB drive.[8]

The Payload Component. It is the mechanism that achieves what a weapons is supposed to do, *i.e.* destroy data, interrupt communications, exfiltrate information, causing computer-controlled centrifuges to speed up as in Stuxnet 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. The exploit itself

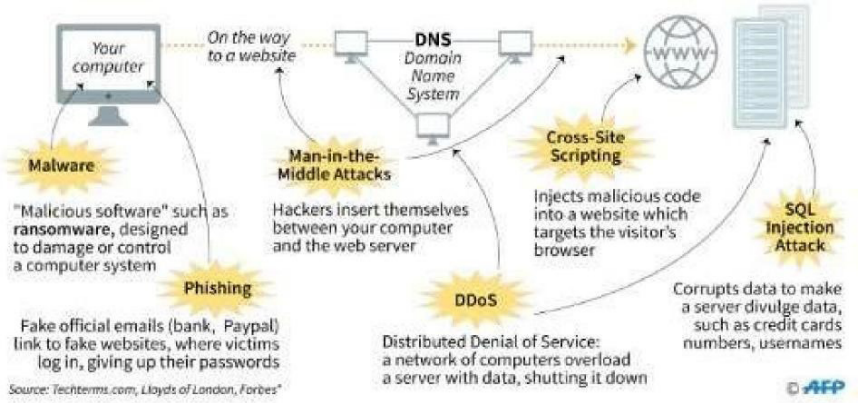
consists of computer code specifically designed to take advantage of a vulnerability to enable the operation of other malware components, such as the payload or further propagation methods. Finally, the payload denotes computer code that is executed on the target system to achieve the attacker's intended goal. The outcome of the payload depend on the technical skills and capabilities of the attacker, the nature of the target and the attacker's intentions. They can vary from exfiltration of data for espionage purposes, to encryption, alteration or destruction of data, to alteration of the functioning of the attacked computer to cause secondary effects on systems or processes controlled by that computer. Finally, it can enable remote access to be controlled or directed over the Internet.

In the following image, the Lockheed Cyber Kill Chain model is shown, which applies to this concept of an attack escalation ladder:



Source: https://www.sans.org/blog/leveraging-the-human-to-break-the-cyber-kill-chain

Weaponisation depends on the quality of intelligence gathered in other operations to identify and develop vulnerabilities, exploits, and propagation methods that would be the most promising.



Source Nicola Bates, Comparing Cyber Weapons to Traditional Weapons Through the Lens of Business Strategy Frameworks, Information Security Group , Royal Holloway, University of London

Characteristics of Cyber Weapons

Some of the unique features of cyber weapons and their operation in cyber space are:-

- It is difficult to distinguish between instruments used to gather intelligence and inflict damage. Usually, the same techniques are used to gain access to an adversary's systems and networks for intelligence gathering and for causing harm. Even if an adversary detects a penetration, cannot be sure of the penetrator's intent. It may misinterpret an attempted intelligence operation as an attack.

- OCO act on intangibles. Information, knowledge and confidence through cyber operations can cause tangible effects. OCO are deceptive.

- The efficiency of a cyber weapon is a vital function of the target's characteristics. Even a small change in the target machine's configuration, system or network can negate the effectiveness of a cyber weapon against it. For OCO, this extreme 'target dependence' requires that intelligence information on target characteristics must be precise, high-quality, high-volume, current and available at the time of the weapon's use.

- A prerequisite for an attack's success is interaction with the target in advance of an actual cyber attack. The attacker may have secretly installed a 'back door' that will grant the attacker access later for downloading a customised attack payload.

- Military planning often entails drawing up lists of well-known and understood targets—military stations, logistic installations including ammunition and fuel storage facilities, telecommunications facilities, etc. In comparison, many targets in cyberspace can appear and disappear from the internet with the flick of a switch.

- Cyber weapons can buy time for policymakers who are faced with the need for immediate action.

- Designing a cyber weapon so that it can be used in a targeted manner is technically demanding. With precise intelligence about the targets, it is possible to conduct cyber-attacks that are specifically targeted to achieve the desired effect and with minimal damage to entities that should remain unharmed.

- Proliferation of cyber weapons. A cyber weapon, once used, may become available for others to examine, copy and reuse for their purposes. The Shadow Brokers revealing National Security Agency (NSA) hacking tools is an example of cyber weapon proliferation.

- Compared to a conventional military, the barrier to entry is very low. Encryption algorithms are readily available. Attackers can purchase highly customisable Ransomware-as-a-service (RaaS) subscriptions for as low as $40 per month.

There is unpredictability and potential for collateral damage associated with their use. Due to the ever-changing innovations in enterprise architecture and network operations and IT interdependencies, predicting the precise effects of an attack are very difficult. As in other warfighting domains, an actor may have conducted intelligence, surveillance, and reconnaissance (ISR) operations and mapped out vulnerabilities in an adversary's cyber network. However, unlike in the conventional realm, the targeted actor can flip a switch and

instantly change the target network or even unplug it altogether.

The question of using cyber weapons is controversial. When the nation-states and other actors start to use offensive cyber capabilities, there is always the possibility of escalation. Unexpected side effects may occur when releasing cyber weapons. Reasons for possessing cyber weapons are:-

- If a state wants to be a credible power, one must have offensive capabilities. One cannot have a credible cyber defence without offensive abilities.

- Offensive capabilities represent the key component of deterrence. The ability to act offensively gives a strong preventive message to the adversaries, provided they understand and believe it.

- Without offensive cyber abilities, no country can build an effective and credible cyber defence. By aggressive thinking, one can understand how the attacker acts and find all possible vulnerabilities in their defence. It helps to test the current defence and training one's forces.

- In contemporary warfare, agility and the concept of operations for smart defence are essential for most countries. One has to be an active defender and snatch the initiative when it is needed. Passive defence alone will not work.

- One cannot defend with kinetic weaponry against a non-kinetic attack.

Comparisons of Cyber and Conventional Weapons

Cyber weapons have some unique features, like the ability to cause damage falling short of triggering kinetic retaliation amongst nation-states to make them desirable. There is the probability for damage done to be reversed, a degree of plausible deniability and an ability to amplify the effects of other traditional capabilities.

These properties show that cyber weapons can offer a particular form

of conflict. Madeline Carr in her book on US Power and the Internet, notes, 'Whilst a material view of power and technology may have been useful in understanding the dynamics at work in conventional conflicts and the nuclear age, *IT lends itself to unconventional conflict characterised by anonymity, geographical dislocation, asymmetry, previously less significant actors on par with states and the interdependence of industrialised states in a vulnerable global network*.[9]

Kinetic weapons typically generate access and effect by force almost instantaneously. Cyber weapons generally separate access and effect into two distinct actions. Often cyber access is developed weeks or months in advance of the intended effect. Cyber weapons require pre-positioning, significant tailoring and/ or bundling with a target-specific access creating capability.

Kinetic weapons produce irreversible physical effects, while cyber weapons can produce completely reversible results. It is problematic to reverse-engineer and reuse kinetic weapons since they are usually damaged beyond reuse. Cyber weapons can also create permanent damage, as was the case of Stuxnet. When a denial-of-service attack stops, the target systems return to normal condition. Encryption used in Ransomware is reversible given the correct decryption key. Ransomware relies on reversibility to be effective. There is a chance that the cyber weapon will be copied intact and studied by an adversary, even if the capture itself is after the attack and used by them.[10]

In conventional war, weapons platforms can be kept at a distance from their target and protected from harm. Ammunition from kinetic weapons is expendable. Once expended, it is difficult or pointless to reconstruct and replay. The number of kinetic payloads delivered in an area can be increased. However, there is a correlation between payload mass, velocity and kinetic effect. A single cyber weapon could be used against one or many targets simply by coding the weapons effects, thus enabling inherent and impressively responsive scalability.

There is a lot of experience in the development, analysis and use of kinetic weapons. Most have evolved slowly over decades or centuries of refinement and application. No such structure exists for cyber weapons. Armed forces have extensive experience in training and employing kinetic weapons.

Cyber weapons do not have the same amount of experience. Hesitance and uncertainty about integrating cyber as a strategic weapon will remain.

Use of force is the last choice for modern conflicts. The *intent behind the use of kinetic weapons is unambiguous. However, cyber weapons can convey ambiguous messaging*. Cyber weapons can be mainly effective when employed below the level of armed conflict.[11] *Continuous global grey zone conflict in cyber domain is likely to occur in the foreseeable future*.

Kinetic weapons are not employed outside of armed conflict. In June 2019, U.S. Cyber Command (USCYBERCOM) carried out cyber attacks against Iran in response to Iranian aggression.[12] The cyber option was executed because the U.S. decided not to exercise kinetic options. This incidence shows that cyber was a less escalatory, non-kinetic option.

Today's military leaders have great confidence in kinetic weapons because of experience and training. Cyber weapons bring mixed confidence in the effects and effectiveness of the weapons. Cyber has recently emerged as a complete instrument of power.

In 2018, the Defense Science Board (DSB) Task Force on Cyber as a Strategic Capability determined that the Department of Defence (DOD) "must move beyond tactical applications for cyber and realise cyber as a strategic capability."[13]

Table. Differences Between Kinetic and Cyber Weapons

	Kinetic Weapons	Cyber Weapons
Weapon	Generate access	Leverage access
	Difficult to reverse-engineer and repurpose	Use may result in others adopting it too
	Permanent effect	Potentially reversible effects
	Local effect	Possible global effect
	Consistent effect	Variable effect
	Scale with volume	Scale with use
	Fixed effect	Tailorable effect

	Fixed effect	Tailorable effect
	Predictable effect and effectiveness	Sensitive to environmental changes
	High barriers for entry	Low barriers for entry
Targeting	One weapon, one target	One weapon, many targets
	Minimal geographic prepositioning	Can be significant prepositioning (system-specific)
	Positive control	Opportunistic
	Coarse targeting	Surgical targeting
Policy and Practice	Significant experience	Little experience
	Unambiguous intent	Potentially ambiguous intent
	Limited value below level of armed conflict	Useful in all levels
	Overtly attributable	Tailorable attribution
	Confident	Mixed confidence

Unique Characteristics of Cyber Weapons [14]

Cyber warfare involves many unique characteristics that do not apply to conventional war. These include *attribution, target and weapon unpredictability, the potential for significant collateral damage or unintended consequences, multi-use nature of the associated technologies, attractiveness to weaker powers and non-state actors as an asymmetric weapon, the use of covert programs for development and the use as a force multiplier for conventional military operation, and finally, questionable deterrence value*.[15]

Challenge of Attribution. It is very difficult to conclusively determine an attacker's origin, identity, and intent if the actor wishes to remain anonymous. Defenders usually lack the tools needed to trace an attack back to the actual attacker reliably.

Multi-use nature of Internet Technologies. Cyber IT systems are multi-use. They may have defence and civilian applications. Many IT and

hardware and software components used for cyber warfare are ubiquitous, commercial, off-the-shelf technologies with many peaceful applications.

Unpredictability and Potential for Collateral Damage. Predicting the precise effects of an attack is very difficult because of the ever-changing innovations in enterprise architecture and network operations and IT interdependencies.

Questionable Deterrent Value. The unreliable effects of cyber weapons, availability of defences and the need for secrecy and surprise reduce their ability to serve as a strategic deterrent. While cyber weapons can inflict unacceptable damage against an adversary, they are possibly unable to offer states an assured capability for doing so.

Importance of Secrecy and Surprise. To develop cyber weapons, covert programs are used. Due to the sensitivities of cyber weapons, their development and availability are not acknowledged or demonstrated. The potential emergence of revolutionary technology like a quantum computer would render all forms of encryption obsolete. The first nation to develop and field a full-blown quantum computer could completely dominate cyber space for a period of time. Smaller technological advances could also have a dramatic effect on the balance of power in cyber space.

Asymmetric Weapon. Weaker powers and non-state actors find cyber weapons attractive as asymmetric weapons. Cyber weapons are attractive to relatively weaker actors (state and non-state) due to their low cost compared to other weapons.

Force Multiplication. Cyber weapons are well-matched for attacks on logistical networks, reinforcements, and command and control facilities to induce operational paralysis, reducing the enemy's ability to move and coordinate forces in the theatre. Cyber weapons can provide an attacker with the capability of seizing valuable natural resources or industrial facilities without risking their destruction.

Volatility. With physical attacks, it is possible to predict its effects on the ground. With cyber weapons, it may be difficult or impossible to predict the weapon's effect or to determine the impact after the event.

Offence Dominance. Within the cyber domain, the offence has the upper hand. The perception that cyber is offence-dominant has led to nation-states building up cyber capability in a race for dominance.

Under Theorisation. Ben Buchanan in his 2020 book 'The Hacker and the State' states that cyber capabilities are non-intuitive and not as dependable, fungible, or retargetable as traditional arms. Finding that while most policymakers and scholars understand what nuclear weapons and tanks can do, the possibilities, pitfalls, and processes of hacking missions are comparatively opaque.

Cost. Cyber weapons cost more in research and development. However, simple tools like the $25.95 off-the-shelf software used by Iraq in 2009 to capture video feeds from U.S. drones can cost just a few dollars. At the same time, zero-day vulnerabilities for an iPhone can cost over $2 million. The cost of cyber weapons would include purchasing vulnerabilities, the cost of training and paying the code developers. Cyber weapons are probably getting cheaper due to:-

- Labour gets more efficient as attackers spend less time experimenting, leading to fewer mistakes in code.
- Malware development gets standardised by developers in exploit tool kits, leading to an increase in efficiency.
- Building upon and reusing existing tools and code allows more efficient cyber weapon production - even actors with limited resources can download open-source tools.
- Shared experiences of vulnerabilities, exploits and propagation techniques allow others peoples 'lessons learned to be shared.

Life Expectancy of Weapons. Cyber weapons have a finite life, after which they will not work. A zero-day exploit for the Windows Operating System will eventually be found and patched, or newer versions released, making it useless except in old, unpatched versions. The investment in cyber weapons can be millions of dollars, and they can become ineffective. The average life expectancy of zero-day exploits and their underlying

vulnerabilities is around 6.9 years.

Intrusion and Attack may look the Same. Techniques used to gather intelligence and those techniques used to inflict damage used by cyber weapons are hard to distinguish in real life. If malware is detected on the network, systems administrators cannot be sure of the infiltrator's intent and may misperceive an intelligence operation as an attack. The intent of an intrusion would only be known for sure when the attack has commenced.

Vulnerabilities Equities Process. Countries seeking to use an exploit against an enemy leave themselves open to the same exploit being used against them. The 'Vulnerabilities Equities Process' determines if software vulnerabilities should be disclosed or not. If the government retains vulnerabilities they will go to their cyber arsenal for use in a cyber attack. Disclosures are released to the vendors of the software to patch and pass on to the public. These patches close the vulnerability, preventing the weapon from being used against the vendor's systems worldwide.

Legal Aspects

Cyber weapon performs actions that would, in normal circumstances, require a spy or a soldier to do. It would be considered either illegal or an act of war if performed by a human agent of the sponsor during peacetime. International laws and agreements are applicable for conventional wars. Cyber warfare has blurred the line between nation-states and non-state actors and even between traditional notions of sovereignty and loyalty. The laws of war are a set of international rules and conventions that limit the belligerent's actions in a war or conflict. A group of United Nations experts in 2013 reached a consensus that existing international law applies in the cyber domain.[16]

The U.S. has always insisted that the *Law of Armed Conflict applies to the cyber domain*. The U.S. DoD Law of War Manual explicitly allows offensive operations in cyber space for damaging or destructive purposes as long as they are conducted in accordance with the laws of war.[17] The U.S. DOD Law of Armed Conflict outlines three examples where cyber

weapons could be employed to achieve mass casualties. Specifically, these cyber operations are:-

- Initiate a nuclear plant meltdown.
- Open sluise gates of a dam above a populated area, causing destruction.
- Disable air traffic control services, resulting in aeroplane crashes.

However, other states like Russia and China have queried if the Law of Armed Conflict are adequate, and argue for the development of new, cyber-specific legislation.

To try and bring some international consensus to the cyber domain, the 2013 '*Tallinn Manual on the International Law Applicable to Cyber Warfare*' was written.[18] In 2017, the second edition, 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations', was published. In this new edition, there is a scenario where a cyberattack is used to acquire the credentials, with the intent of threatening to conduct cyber operations against the system in a manner that will cause significant damage or death.[19] It is not a legally binding document. But this new second edition reflects the level of physical destruction cyber attacks can achieve and their growing scope.[20]

In cyber operations, rules of engagement are not clear. Policies and laws governing the use of cyber weapons are still under development. However, cyber space also exists in real space with its essential physical components such as computers, networking equipments, storage devices and human users. As such, activities and users are partly subject to the standard controls of the territorial state - legislature, courts and police forces.[21]

Use of Cyber Weapons

Use of cyber weapons on targets during a conflict or in peacetime can have disastrous consequences. However, there is a growing tendency of their use on the battlefield or in peacetime. U.S. has publicly acknowledged

using cyber weapons in its fight against the Islamic State of Iraq and Syria (ISIS). In February 2016. Secretary of Defense Ash Carter said that the U.S. Cyber Command is conducting offensive cyber operations to cause ISIS to "lose confidence in their networks, to overload their networks so that they can't function, and do all of these things that will interrupt their ability to command and control forces."

No loss of life has been repored directly linked to cyber attacks till date. There is no international agreement on how cyber weapons should be regulated. There is an increasing temptation for nations to view cyber weapons as a form of warfare favouring or even replacing traditional negotiations that can be prolonged or frustrating. The danger is, *the next generation of cyber weapons will increasingly target and destroy physical equipment in industrial and military facilities. Human casualties will not be too far*.[22]

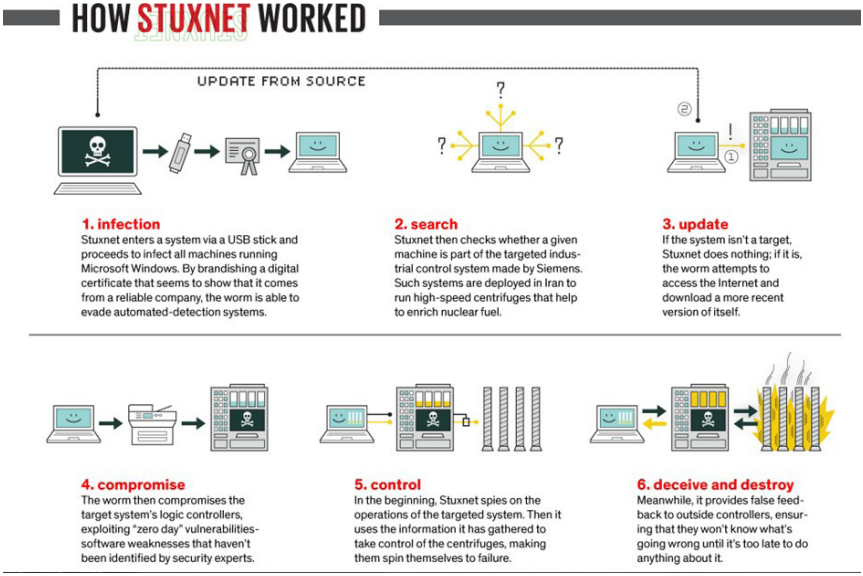
In today's interconnected world, there is a danger of cyber weapons spilling into the open. Such spillage and a black market for malware create new risk vectors. In 2017, the National Security Agency of U.S. lost control of a cyber weapon known as EternalBlue. It was leaked online by a group known as the 'Shadow Brokers'. As states spy on each other, the malware used by them can be repurposed to attack commercial interests, support authoritarian domestic spying campaigns and compromise individual privacy.

Stuxnet

'Stuxnet' was the first example of a cyber weapon being used independently to cause physical damage. It showed the strategic utility of cyber weapons to disrupt, deny and deceive an adversary's strategic intentions. Stuxnet targeted the industrial information systems developed by the German company Siemens which the Iranian government used in some of its uranium-enrichment plants. The Belarusian Company VirusBlokAda detected Stuxnet. There is no official declaration of the Stuxnet worm being a result of any specific country. Analysis of the code of the Stuxnet indicated that the level of complexity required for this type of weapon could only originate from the global superpower in cyber space. NSA of

the U.S. has the capabilities to develop that advanced code to enable a weapon as complex as Stuxnet. Unit 8200 of Israel, have also been named for the Stuxnet attack. It is widely accepted that this was a joint program of U.S. and Israel cyber operators.

Stuxnet was installed on internal systems within the nuclear facility most likely by the contacts that the Central Intelligence Agency (CIA) had in Iran. They were provided with a USB device that contained the early version of Stuxnet. The malware went deep into the core of the Natanz network and found its target: the PLC controllers. PLC controllers control critical functions within the centrifuges that are used for enriching uranium. Stuxnet degraded the facility's ability to further enrich uranium, as the specific speed required for that precise process was impacted.



Source: https://spectrum.ieee.org/the-real-story-of-stuxnet

Stuxnet is a sophisticated cyber weapon that relied on several zero-day vulnerabilities to penetrate systems not connected to the Internet. It had to function autonomously after injection. The makers of stuxnet had very precise knowledge of the target environment. It also manipulated output displays to deceive the plant's operators into believing that the centrifuge

complex was operating correctly.[23]

Although stuxnet damaged the Iranian nuclear program, the attack's overall effect was not impressive. Iran replaced all of its damaged centrifuges and has resumed enriching uranium. This shows that *cyber weapons are not the 'silver bullet' replacement for more-traditional military instruments. It was not able to coerce the Iranian regime into abandoning their program*.

Different variants of the Stuxnet were found in different organisations across the globe For the next seven years. 'Duqu', a separate but closely technically-related version of Stuxnet, was discovered in 2011. Another closely tied technical variant of Stuxnet, Flame, was discovered in 2012. In 2017, Triton, yet another variant of Stuxnet's original tooling, was found lurking in in petrochemical plants that used Siemens S7 PLC controllers. The variants of stuxnet were not exclusive to the US or its allies.

Shamoon

Iran retaliated for Stuxnet by attacking the Saudi Aramco oil company with a cyber weapon, named 'Shamoon'. It hit without warning and within hours had taken over the network and erased the disks of infected computers. The malware was apparently installed by an insider in the corporate network and not in a separate, disconnected net that ran the oil production machinery. Shamoon spread via shared network drives. It limited its spread to within the targeted corporation.

There has been other instances of cyber weapons being used like North Korea's 'Sony' attack or Russia's attack multiple sites in the power grid in Ukraine etc. These are not discussed here.

Examples of some of the attacks by cyber weapons are given below:-

Approx date	Target	Source	Motivation	Actions
April 2007	Estonia	Not attributed, widely thought to be hackers operating from Russia	In retribution for Estonia's decision to relocate a Soviet-era war memorial (and perhaps more controversially, but significantly less reported, the bodies of soldiers from the Red Army30) from central Tallinn to a war graves cemetery outside the city.	Series of attacks by patriotic hacktivists, sustained over three weeks; multiple DDoS attacks against Estonian utilities, telecommunications and government facilities
August 2008	Georgia	Not attributed, but thought to be the work of Russian Business Network and the South Ossetia Hack Crew	In support of Russia's military incursion into South Ossetia.	Attacks on 38 sites, mostly Georgian and embassies of the US and the UK; DDoS, site defacements, traffic re-routing
June 2009 – July2010; discovered June 2010	Iran	Not attributed, but thought to be a joint operation between the US and Israel	To derail / delay Iran's nuclear programme.	Delivered Stuxnet, caused physical damage to uranium refining operations at the Natanz nuclear facility. Iran was later the target of 'Flame', a very large malware discovered in June 2012 but later found to be operational since at least 2010.
2014 – current; December 2016	Ukraine	Not attributed, but thought to the work of Cyber Berkut and Sandworm Team pro-Russian hacktivists	In support of Russia's claim on Crimea, invasion of March 2014.	DDoS attacks against NATO, Government of Poland and the Ukraine Government; attacks on Ukraine's power grid disrupted electricity supplies to at least 100,000 people

Approx date	Target	Source	Motivation	Actions
6 September 2007	Syria	Israel	As part of the ongoing Israel-Syria conflict.	'Operation Orchard' hijacked Syrian airspace control imagery; provided cover for an airborne attack and destruction of a nuclear power facility under construction in the Dayral-Zawr region
2010	Afghanistan	US	As part of ongoing US-led campaign in Afghanistan.	Expeditionary cyber-support unit deployed as part of combat operations
April 2013	US	Claimed by the Syrian Electronic Army	To discredit the 'western' media.	Used fake Twitter account to erroneously report 'two explosions in the White House and Barack Obama is injured'; Dow Jones Stock Exchange dropped 70 points, but quickly recovered when the news was proven false.

Source: Carr (2011); Green (2015); Solis (2014); UK MoD (2016); Dannanberg (2016); Zetter (2016))

The Shadow Brokers

Emergence of 'The Shadow Brokers' provided a new dimension to cyber weapons. The Shadow Brokers, on August 13, 2016, posted a Pastebin notice that stated that they had procured, via unknown means, access to specific tools that came from the Equation Group. The Equation Group is known to be part of the elite Tailored Access Operations team of the NSA and is thought to be directly responsible for the design and deployment of Stuxnet.

This Pastebin notice started with the a text, "Equation Group Cyber

Chase Weapons Auction – Invitation!!! Attention government sponsors of cyber warfare and those who profit from it !!!! How much you pay for enemies cyber weapons? Not malware you find in networks. Both sides, RAT+ LP, full state sponsor tool set? We find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic. We find Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons. You see pictures. We give you some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But not all, we are auction the best files."

The posting follows up with, "The Pastebin continues with instructions for obtaining the password to the encrypted auction file. Auction Instructions:

We auction best files to highest bidder. Auction files better than stuxnet. Auction files better than free files we already give you. The party which sends most bitcoins to address: 19BY2XCgb De6WtTVb TyzM9e R3LYr6VitWK before bidding stops is winner, we tell how to decrypt. Very important!!! When you send bitcoin you add additional output to transaction. You add OP_Return output. In Op_Return output you put your (bidder) contact info. We suggest use bit message or I2P-bote email address. No other information will be disclosed by us publicly. Do not believe unsigned messages. We will contact winner with decryption instructions. Winner can do with files as they please, we not release files to public."

The Shadow Brokers, following that posting on Pastebin in October 2017, would again post that they had access to specific NSA-level tools built or used by the Equation Group. The most important leak by the Shadow Brokers emanated in April of 2017 when they posted a tweet linked to their @Shadowbrokers account. It gve out the links to codeword exploits. The most potent of these was 'EternalBlue'. Over 200,000 machines were infected within the first two weeks of its posting online. In the 'NotPetya' and 'WannaCry' Ransomware attacks that followed, leftovers of the EternalBlue exploit appeared, Millions of machines were affected and billions of dollars of loss would be incurred by organisations all over the world.

Specific motivations behind the Shadow Brokers are not known. Till date, there has been no owner of the Shadow Broker leaks. Edward Snowden stated on his Twitter feed that "circumstantial evidence and conventional wisdom indicates Russian responsibility". It was not validated. Irrespective of who the Shadow Brokers were - Russian moles, nation-state hackers, disgruntled employees or political activists - it is a fact that it was the equivalent of tactical cyber weapons being offered freely to everybody inteested on the planet.

Recent Attacks

The recent attacks by cyber criminals on 'SolarWinds' and attack on Microsoft exchange show new progress to cyber weapons that have national security implications.

SolarWinds

SolarWinds, a major US information technology firm, was subjected to a cyber attack that spread to its clients and went undetected for months. FireEye, an elite cyber security firm, announced On December 13, 2020, the discovery of a highly sophisticated cyber intrusion that leveraged a commercial software application made by SolarWinds. The advanced persistent threat (APT) actors infiltrated the supply chain of SolarWinds, inserting a backdoor into the product. As customers downloaded the Trojan Horse installation packages from SolarWinds, attackers could access the systems running the SolarWinds products.

This cyber attack was exceptionally complex and continues to evolve. The professional competence displayed by the attackers was nonpareil.[24] The hackers also found their way into the Cyber Security and Infrastructure Security Agency, or CISA , whose job is to protect federal computer networks from cyber attacks as part of the office at the Department of Homeland Security . Microsoft Corp President Brad Smith said, "It is the largest and most sophisticated attack the world has ever seen. I think from a software engineering perspective, it's probably fair to say that this is the largest and most sophisticated attack the world has ever seen. When we analyzed everything that we saw at Microsoft, we asked ourselves how

many engineers have probably worked on these attacks. And the answer we came to was, well, certainly more than 1,000."[25]

U.S. agencies including parts of the Pentagon, the State Department, the Department of Homeland Security, the National Nuclear Security Administration, the Department of Energy and the Treasury were attacked. So were private companies like Microsoft, Intel, Cisco and Deloitte, and other organisations like the California Department of State Hospitals and Kent State University.[26] The attack was done so stealthily that it went undetected for months. Security experts feel that some victims may never know if they were hacked or not.

Federal investigators and cyber security experts of U.S. believe that SVR, known as Russia's Foreign Intelligence Service, is probably responsible for the attack. Russia has denied any connection with the breach. Former President Donald Trump had suggested, without evidence, that Chinese hackers may be the culprits.

The breach came as a wake-up call for federal cyber security efforts. The National Security Agency and the military's U.S. Cyber Command were also caught flat-footed. They received billions of dollars in funding to protect American networks and was "blindsided" by the attack. Instead, FireEye, a private cyber security firm, was the first to notice the breach when it saw that its own systems were hacked.

In normal course, NSA's cyber operators sit in foreign networks looking for signs of cyber attacks before they happen. Critics said NSA should have seen the SVR, preparing for this attack. The SVR has a good understanding of what the NSA is looking for. SVR could make the transition from wherever they were operating into the U.S. networks. The hackers didn't do anything elaborate to give them the domestic footprint. They only rented servers from Amazon and GoDaddy.[27]

Attack on Microsoft Exchange Server

As the attack on SolarWinds were being revealed, another major hack hit the Microsoft Exchange Server. Like SolarWinds, it also impacted the federal government. On March 2, 2021, Microsoft reported that at least

30,000 customers were affected by a cyber attack that allowed outsiders to access the firm's email and calendar service through a software loophole previously unknown to the company.[28] Microsoft concluded that the attacks were originated from China and appeared to be state-sponsored.[29] Microsoft identified the group behind the hack as a relatively unknown Chinese espionage network dubbed Hafnium.

Microsoft disclosed that Chinese nation-state actors exploited four vulnerabilities in its on-premises email server software. Patches were released. Though attacks were initially thought to be limited, it was not so. An emergency directive was issued shortly after from the Cyber Security and Infrastructure Security Agency (CISA), warning all government civilian departments and agencies to update immediately.

On July 19, 2021, the U.S. justice department charged four Chinese nationals with hacking. U.S. accused Beijing of extortion and threatening national security. The secretary of state, Antony Blinken, accused China of being responsible and said it was part of a "pattern of irresponsible, disruptive and destabilising behaviour in cyber space, which poses a major threat to our economic and national security. Ministry of State Security (MSS) has fostered an ecosystem of criminal contract hackers who carry out both state-sponsored activities and cyber crime for their financial gain. As evidenced by the indictment of three MSS officers and one of their contract hackers unsealed by the Department of Justice today, the United States will impose consequences on [Chinese] malicious cyber actors for their irresponsible behaviour in cyber space."[30] The U.S. administration and its allied nations disclosed a range of other cyber threats from Beijing. It included Ransomware attacks from government-sponsored hackers that have targeted companies with demands for millions of dollars. The MSS of China has been using criminal contract hackers, who have engaged in cyber extortion schemes and theft for their own profit.

The E.U. and Britain also pointed the finger at China. The E.U. said malicious cyber activities with significant effects that targeted government institutions, political organisations and critical industries in the bloc's 27 member states could be linked to Chinese hacking groups. E.U. foreign policy chief Josep Borrell said the hacking was "conducted from

the territory of China for the purpose of intellectual property theft and espionage." U.K. Foreign Secretary Dominic Raab said that the Microsoft Exchange cyber attack "by Chinese state-backed groups was a reckless but familiar pattern of behaviour."

China was quick to react. The next day, on July 20, 2021, China's foreign ministry spokesperson, Zhao Lijian, hit back at the US-led allegations, calling the campaign purely a smear and suppression with political motives. He accused the CIA of conducting cyber attacks on China's aerospace research facilities, oil industry, internet companies and government agencies over 11 years. He said, "China once again strongly demands that the United States and its allies stop cyber theft and attacks against China, stop throwing mud at China on cyber security issues and withdraw the so-called prosecution." Zhao stated that the U.S. launches the largest number of cyber attacks worldwide each year, citing a 2020 reportof Chinese internet security firm '360' that supposedly found the CIA as the culprit behind the hackings of vital Chinese companies and government institutions for more than a decade.[31]

Ransomware

Ransomware is a type of malware which is used to deny access to IT systems or data. After the initial infection, the Ransomware attempts to spread to shared storage drives and other accessible systems. The hackers demand payment, from victims to regain access to an infected device and its stored data often via Bitcoin or prepaid credit card. If the Ransomware criminals' demands are not met, the system or encrypted data remains unavailable. The data may be deleted or released publicly. The flourishing growth of Ransomware can be ascribed to the ease of deployment and a high return on investment. Criminal organisations are progressively relying on such attacks to generate profits.

Encryption has its limitations. As Ransomware relies on denying access, encryption cannot inflict costs if the victim doesn't value what's being encrypted or can easily replace the asset. A defender has an alternative way to get their data back after a Ransomware attack if it can adopt real-time, offline backups.

According to the U.S. Department of Homeland Security (DHS), attacks using Ransomware have at least doubled since 2017. The criminal groups are targeting U.S. critical infrastructure. Risks from attacks on these critical systems and assets include national security, economic stability and public health and safety. Seeing the gravity of the situation, individuals representing more than 40 organisations in the public and private sectors collaborated to produce an 81-page report outlining recommendations for the U.S. government and private companies alike on how each can avoid and address Ransomware attacks. The list of technology companies that contributed to the report includes Microsoft, Amazon Web Services, McAfee, and FireEye. The coalition included, from the public sector, experts representing the CISA, FBI, the National Governors Association and the U.S. Secret Service, among others.

The Ransomware task force estimated that payments to Ransomware cryptocurrency accounts reached $350 million in 2020, a 311 percent increase. Total losses, including downtime and remediation, are forecast to reach $20 billion this year. One analysis identified 304 million Ransomware attacks worldwide in 2020, a 62 percent increase from the previous year. Recorded Future, a security firm that tracks Ransomware attacks, estimated that there were 65,000 successful Ransomware attacks last year, or one every eight minutes.

Recent Ransomware Cases

In 2017, the global WannaCry attack revealed the impact Ransomware could have on people's everyday lives when National Health Service hospitals across the U.K. fell victim to the attack. Appointments had to be cancelled, and people who came for treatment were sent back. About four years later, the problem of Ransomware has got worse. In a speech on March 31, 2121, Homeland Security Secretary Alejandro Mayorkas described Ransomware as a threat to national security.

In October 2020, U.S. Department of Justice announced that six Russian individuals were indicted for NotPetya Ransomware causing nearly $1 billion in losses to the three known victims identified in the indictment. NotPetya, was a type of malware that exploited existing vulnerabilities in

computer software or networks. It encrypted files and allowed attackers to gain privileged making the infected Windows computers unusable. In December 2020, U.S. federal law enforcement received several reports of Ransomware attacks against K-12 educational institutions. Malicious cyber actors targeted school computer systems, slowing access and, in some cases, rendering the systems inaccessible for essential functions, including distance learning.

In January 2021, U.S. Department of Justice announced a coordinated international law enforcement action to interrupt a sophisticated form of Ransomware known as NetWalker. In February 2021, the Department of Justice announced that three North Korean individuals were indicted for creating the destructive WannaCry Ransomware and the extortion and attempted extortion of victim companies from 2017 through 2020. In May, 2021, one of the largest healthcare providers in the U.S., Universal Health Services, was affected by a Ryuk Ransomware attack that left hospitals nationwide unable to access critical systems for weeks during the COVID-19 pandemic. In June 2021, the White House announced that the world's largest meat processing company, JBS, had been targeted with Ransomware affecting the company's operations. The company paid $11 million in ransom.[32]

On America's independence day of fourth July this year, the 'REvil' Ransomware gang locked up the data of more than 1,000 businesses in an unprecedented supply-chain attack on the software firm Kaseya, demanding $70 million for the data's release. REvil, a major Russian-speaking Ransomware syndicate, is among Ransomware gangs that steal data from targets before activating the Ransomware. Active since April 2019, the REvil provides Ransomware-as-a-service. It develops the network-paralysing software and leases it to its affiliates who infect targets and earn the lion's share of ransoms. In a recent report, the Palo Alto Networks cyber security firm stated that the average ransom payment to the group was about half a million dollars last year.[33]

'Colonial Pipeline', a major conduit for fuel delivery for much of the East Coast, on May 8, 2021, announced that it was the victim of a Ransomware attack that led to a temporary disruption in the distribution of gasoline

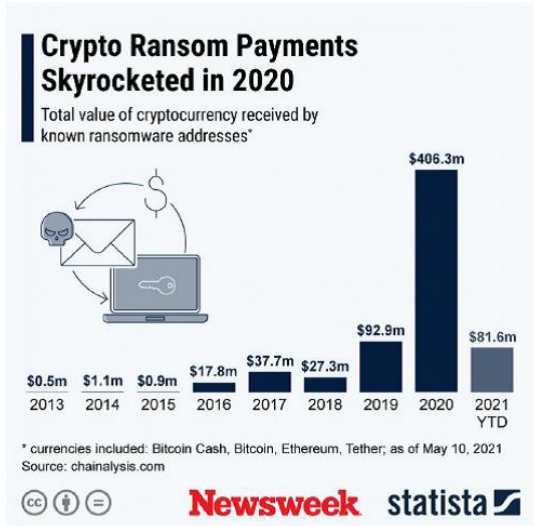
and other petroleum products across most of the southeast U.S. It had temporarily shut down all pipeline operations as a precautionary measure. Joseph Blount, CEO of Colonial Pipeline Co. confirmed that he had authorised a ransom payment on May 7, just hours after the cyber attack. Colonial paid a ransom of 75 bitcoin, then valued at USD 4.4 million. A week after the attack, once Colonial paid a ransom of $4.4 million to get its systems back online, eighty per cent of gas stations in Washington, D.C., still had no fuel.

On May 10, 2021, the FBI released a statement confirming that "the 'Darkside' Ransomware is responsible for the compromise of the Colonial Pipeline networks." Colonial's payment wasn't the largest ransom paid by a single organisation. Last year, the maker of the popular fitness tracker, Garmin,reportedly paid a record $10 million in ransom. The U.S. government recovered more than $2 million of cryptocurrency that Colonial Pipeline paid in ransom to the Russia-based hacker group DarkSide after authorities could locate the private key that unlocked a digital "wallet" holding the ransom payment[34]. The operation to get back cryptocurrency reflected a rare victory in the fight against Ransomware.

Cyber Operations and Impact

Operation	Severity	Scale	Duration	Specific
NotPetya	High: data destruction	Global. Affected organizations in Europe, the US and Asia (Maersk, Merck, Rosneft, Beiersdorf, DHL, and others) but also a concentration in Ukraine (banking, nuclear power plants, airports, metro services).	Short-term, with recovery spanning over months to a year.	No
WannaCry	High: data destruction	Global, but primarily in Russia, Ukraine, India and Taiwan. Operation affected multinationals, critical infrastructureand government.	Short-term, with recovery spanning over months to a year.	No

Operation	Severity	Scale	Duration	Specific
Destover	High: data destruction	Focused on Sony Pictures Entertainment (<7,600 employees), a subsidiary of Sony Corporation (131,700 employees in 2015).	Short-term, with recovery in months.	Yes
Stuxnet	High: destruction of centrifuges	Focused on Iran's nuclear weapon development program.	<1 year	Yes
Various offensive cyber operations against ISIS by US, Australia, UK	Varied: some data destruction but also denial and manipulation effects	Focused on Islamic State.	Unknown	Yes



A Statista graphic shows the amount of known cryptocurrency payments made in Bitcoin Cash, Bitcoin, Ethereum and Tether from 2013 through May 10, 2021 as compiled by chainalysis.com.STATISTA

The above graphic was provided by Statista.

Implications for National Security

In recent times, Ransomware attacks have shut down or disrupted critical infrastructures. What was previously seen as a nuisance is fast becoming a significant risk to national security as cyber criminals target vital parts of

the country's infrastructure. A group of attackers intending to inflict havoc could quietly infect a series of critical systems and then simultaneously cripple many essential elements of infrastructure.[35]

Rep. Michael Waltz (R-Fla.), a member of the House Armed Services Committee, said, "At the end of the day, I don't think the American people really make these legalistic distinctions between criminal and state-sponsored attacks. An attack on our oil infrastructure or food supply is an attack, period, whether it's from a saboteur planting a bomb, a plane dropping a bomb or a cyber attack."[36]

Kevin Mandia, CEO of the cyber security firm 'FireEye' stated, "When you think about the conflict, you have air, land and sea and space and now cyber. But in cyber, the private sector is front and center. Any conflict in cyber space, whether motivated by a criminal element or motivated by geopolitical conditions, it's going to involve both the government and the private sector. And that response, because it impacts both, you almost need a triage that both sides, both private and public sector, benefit from similar to the NTSB." Mandia envisages a review board for significant incidents where intelligence is gathered and the nation finds a way to defend itself appropriately. Presently, the onus is on private companies to do all the investigations.[37]

Ben Buchanan states that the most significant difference between the cyber domain and the other domains is the role of the private sector. He observes that governments do not have the levers in cyber space needed to solve cyber conflicts. Governments seek private sector cooperation and council in many circumstances, such as from Microsoft, Fire Eye and Crowd Strike. They have more subject matter expertise in this arena, have better access to data from private networks and users and are more agile. As 85 percent of critical infrastructure is in private hands, the private sector owners of this infrastructure are needed for things to get done.

As part of the ongoing response, agencies across the U.S. government announced new resources and initiatives to protect American businesses and communities from Ransomware attacks. The U.S. DHS and the Department of Justice (DOJ), together with federal partners, have launched a new website to combat the threat of Ransomware. *StopRansomware.*

gov establishes a one-stop hub for Ransomware resources for individuals, businesses and other organisations.[38] Secretary of Homeland Security Alejandro N. Mayorkas said, "As Ransomware attacks continue to rise around the world, businesses and other organizations must prioritize their cyber security, Cyber criminals have targeted critical infrastructure, small businesses, hospitals, police departments, schools, and more. These attacks directly impact Americans' daily lives and the security of our Nation. I urge every organization across our country to use this new resource to learn how to protect themselves from Ransomware and reduce their cyber security risk."

Now Ransomware is treated mainly as a criminal problem. Soon it may become a geopolitical issue. The incentives built into Ransomware attacks will make it easier for smaller, poorer players to extract concessions from more powerful adversaries. Ransomware attacks are easier to execute than other forms of geopolitical coercion. Compared to conventional military operations, the barrier to entry is very low. Encryption algorithms are readily available. Attackers can purchase highly customisable Ransomware-as-a-service (RaaS) subscriptions for as low as $40 per month. These practical benefits would seem quite attractive to an impoverished and isolated state or a non-state actor with few resources.

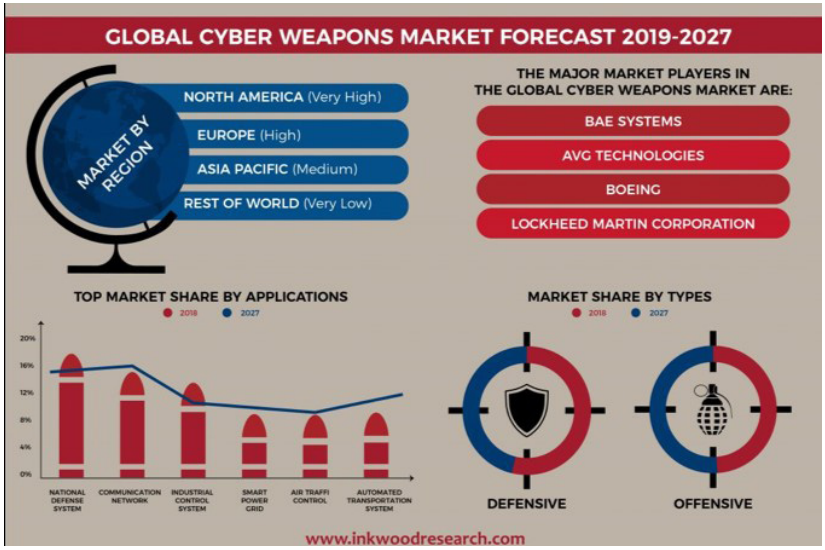
In the current conflict scenarios unfolding worldwide, sooner than later, Ransomware is likely to appear as an additional tool in the toolbox of both state and non-state actors as they seek new ways to make gains without blatantly inviting retaliation. They have less to lose as they are less reliant on cyber space for everyday activity. *It is highly probable that an adversary, a non-state actor, a terrorist organisation or a combination of these hire some Ransomware vendors to carry out attacks together with conventional operations or any major operations to create massive confusion*.[39]

Cyber Weapon Market

Malicious code is available and can be traded and sold on the Dark Web by those with the resources to purchase it or in exchange for illicit products and services. Cyber weapons are cheap and widely available in the market at a price for nation-states and criminals and harmful actors. According

to a study from the University of Maryland, American computers are attacked every thirty-nine seconds.[40] Non-state developers of cyber weapons are engaged continuously in research and development, creating new exploits. It is easy to buy malware to support blatant cyber attacks. Traditional arms control methods are difficult to enforce as cyber weapons are not in the exclusive control of nation-states.

The global cyber weapon market was valued at $45.12 billion in 2018, with this estimated to be worth $65.13 billion by 2027. There is a rising demand for offensive cyber tools and systems. It is predicted to rise as much as 39 percent by 2027. This trend has led cyber experts to call it a 'cyber arms race', which is expected to expand shortly. Finnish IT expert Mikko Hypponen stated that "we might very well be spending the next 60 years in a cyber arms race." The most advanced companies like BAE Systems, CISCO Systems or Israeli Aerospace Industries(IAI) in this field are mainly located in the United States, Israel and Europe.



Source: Cyber Weapons: The New 'Arms Race'? September 3, 2019, https://finabel.org/cyber-weapons-the-new-arms-race/

It is difficult for a country with limited cyber resources and infrastructure to buy an off-the-shelf offensive capability from a private sector actor and effectively operationalise it with full-scale military operations. Actors attempting to

base their entire cyber arsenal on market-available tools and services would look more like sophisticated cyber criminals than powerful nation-states. These countries would not be able to keep up with advanced players already possessing sophisticated internal capabilities. A more powerful state can easily acquire the same readily available off-the-shelf tool or service. While the novice has to rely solely on the ready-made tools, the expert can integrate it into existing capabilities to build a much more effective campaign.

A real black market of computer vulnerabilities found in the most commonly used software which are not yet publicly known (the so-called 'zero-day' or '0-day') have emerged. The following table indicates the price range for every zero-day detected and put up for sale on this illegal market.[41]

ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50.000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80.000-$200,000
IOS	$100,000-$250,000

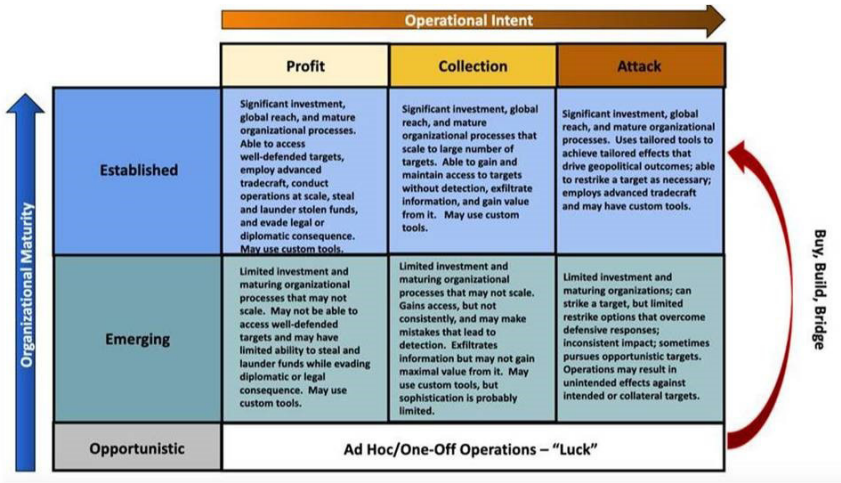
A range of cyber tools is available to the state and non-state threat actors. However, these actors likely will achieve varying degrees of success despite having access to comparable capabilities. One reason is their ability to operationalise cyber capabilities. Advanced organisations would integrate a mix of technical, operational and other skills and develop processes to conduct cyber operations. Operational intent is another factor which spans a range from simple theft to complex operations calibrated to achieve precise and reliable disruptive effects.

Intent can range from profit collection to attack. To conduct a cyber attack that achieves reliable and repeatable impact on critical infrastructure or another target may require understanding how that target operates and

countering defenders' efforts to reconstitute.

Organisational Maturity [42]

Based on increasing levels of organisational maturity, three categories of actors are identified: opportunistic, emerging and established.



The Grand Cyber Arms Bazaar Framework

Source: Commodification of Cyber Capabilities: A Grand Cyber Arms Bazar, Public Private Analytic Excange Program, November,2019 available at: https://nsiteam.com/social/wp-content/uploads/2019/11/191119-AEP_Commodification-of-Cyber-Capabilities-Paper.pdf

Established Actors. Organisations with the most advanced, accurate, and agile tools are considered established actors. They have extensive resources, including time and money, to achieve persistence and achieve global reach. Established actors use malware like 'Zebocry' to target diplomats, defence officials and ministry of foreign affairs staff to steal login credentials, keystrokes, communications, and sensitive files.[43] When these tools are deployed in synchronisation with military efforts, the scale of impact is significantly broader.[44]

Emerging Actors. Emerging actors include nation-states, criminal organisations and others who have defined processes, capabilities and a history of targeted operations. Their attempts are not consistently

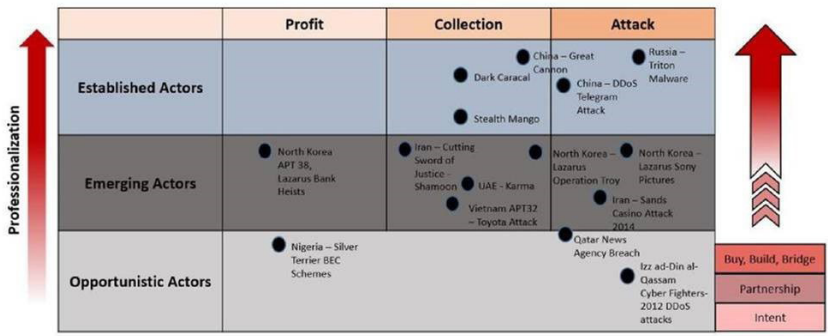
successful. Impacts are inconsistent. They have no immediate restrike capabilities. Some of these actors are technologically less capable than the established actors. They look to global powers such as China and Russia for concepts. These concepts and resources provided by established powers could lead a low-level actor to become an emerging threat.[45]

Opportunistic Actors. Opportunistic actors are connected with low-level cyber criminal activity. They continuously innovate to keep pace with current trends and avoid law enforcement intervention.[46] Though often leveraging open source tools or existing code, some cyber criminals are now using more sophisticated tools and techniques developed and leaked by other actors.[47]

Another expert differentiated offensive cyber capabilities by three components:-

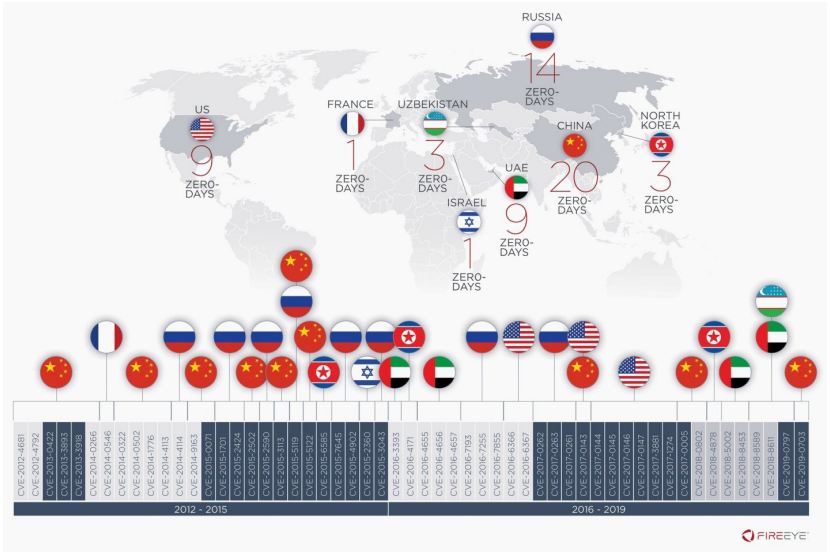
- **People**. Operators, developers, system administrators, front office personnel, strategic and legal experts, etc.
- **Exploits and tools**. Their origination and usage
- **Infrastructure**. Degree of outsourcing of cyber infrastructure

This is illustrated in the figure below:-



Source: Commodification of Cyber Capabilities: A Grand Cyber Arms Bazar, Public Private Analytic Excange Program, November,2019 available at: https://nsiteam.com/social/wp-content/uploads/2019/11/191119-AEP_Commodification-of-Cyber-Capabilities-Paper.pdf

Today, in another interesting development, former government, intelligence or military cyber experts offer their expertise for hire to nation-states seeking to start cyber programs. The government of the United Arab Emirates (UAE) employed former U.S. government intelligence personnel working for Dark Matter to boost the government's cyber abilities. Dark Matter, the contractors, may have operated at a level close to top-tier national security agencies. It leap frogged the UAE's cyber abilities quickly and significantly to achieve hard-to-obtain goals in cyber space previously. Now commercial firms are offering sophisticated cyber capabilities to foreign governments or customers for sale. The unstable military regime may use it against an adversary or its own citizens.[48] FinFisher, a Germany based private company, developed a know-how that has been extensively used and exported. As per Citizen Lab, there have been 33 likely government users of FinFisher in 32 countries."[49,50]



Collection of countries using Zero days

Source : https://www.wired.com/story/zero-day-hacking-map-countries/?bxid=5be9d4c53f92a4046 9e3 7a53&cndid=49798532&esrc=desktopInterstitial&source=EDT_WIR_NEWSLETTER_0_DAILY_ZZ&utm_brand=wired&utm_campaign=aud-dev&utm_mailing=WIR_Daily_040620&utm_medium= email&utm _so urce=nl&utm_term=list2_p5

About a hundred nations have cyber organisations of some kind, on the lines of U.S. Cyber Command. The funding, number and quality of human resources, organisation, technical capability, willingness to use the weapon, policy etc., may vary. Use of beyond the government resources are different for different countries. The U.S. tends to rely on private contracting companies. Russia has made use of criminal networks. China is linked to its cyber militia.[51]

Cyber Weapon Usage

Policymakers do not thoroughly understand the particular characteristics of cyber weapons and their possible use at the strategic level. Former NSA and CIA director Michael Hayden noted, "From their inception, cyber weapons have been viewed as 'special weapons,' not unlike nuclear devices of an earlier time. But these weapons are not well understood by the kind of people who get to sit in on meetings in the West Wing, and as of yet, there has not been a Herman Kahn [of 'On Thermonuclear War' fame] to explain it to them."[52]

The 'FireEye' argues that proliferation is due to a *rising industry of hackers-for-hire that develop zero-day tools and sell them to intelligence agencies worldwide*. Rather than build, any nation with money can buy, relatively sophisticated hacking abilities. Kelli Vanderlee, the FireEye's Intelligence Analysis group manager, says, "Since about 2017 the field has really diversified. We think that this is at least partially due to the role of vendors offering offensive cyber threat capabilities. The biggest barrier between an attacker and a zero-day is not skill, but cash." FireEye specifically indicates companies like the NSO Group, Hacking Team and Gamma Group as the kind of contractors that have facilitated a new cadre of countries to buy their way into the zero-day hacking field. NSO Group's zero-days have come up in the hands of espionage-focused hacking groups associated with the UAE, like Stealth Falcon and FruityArmor. Some NSO-linked zero-days were also used by a group called 'SandCat', associated with Uzbekistan's intelligence agency known as the SSS.[53]

Notably absent from the list is Saudi Arabia. It used a zero-day vulnerability in WhatsApp to hack the personal phone of Amazon CEO Jeff Bezos. Besides the eight NSA zero-day vulnerabilities leaked by the mysterious Shadow Brokers group and one revealed in the 2017 Vault 7 Dump, the U.S.' hacking tools are also conspicuously missing from the timeline. South Korea is absent too. One of South Korea's hacker groups was recently tied to five zero-days used to target North Koreans. However, that discovery came too late to be included in FireEye's study.

A major *characteristic of cyber weapons is that significantly impacts the logic of deterrence is the uncertainty regarding their effects*. Due to the potential for IT network evolution and IT interdependencies, it is difficult to predict the precise impact of an attack. In cyber space, the targeted actor is capable of literally flipping a switch and instantly changing the network or even unplugging it all together. This factor is a destabilising force as it rewards immediate hostile action to prevent network modification if cyber reconnaissance-targeting intrusions are later detected.

Network inter-dependencies are another dynamic contributing to the potential for the collateral damage that is characteristic of cyber weapons. Because the internet is made up of hundreds of millions of computers connected through an elaborate and organic interwoven network, and it is the backbone of much of the global economy, there is the potential for significant unintended and collateral impacts from cyber action. This inter-connected nature of IT systems has led to real-world collateral damage. For example, the 2007 Israeli cyber attack on Syrian air defence systems as part of Operation Orchard was believed to have also damaged domestic Israeli cyber networks. Fear of this kind of cyber collateral damage has had a profound effect on military planning.[54] As another example, in 2003, the United States was planning a massive cyber attack on Iraq in advance of any physical invasion – freezing bank accounts and crippling government systems. Despite possessing the ability to carry out such attacks, the Bush administration cancelled the plan because the effects would not be contained to Iraq. Instead, it would also have a negative effect on the networks of friends and allies across the region and in Europe.[55]

Uncertain effects of cyber weapons, coupled with the availability of defences and the need for secrecy and surprise reduce their ability to serve as a strategic deterrent in their own right. Available defences and the potential for network evolution to mitigate the effects of an attack given early warning requires cyber attackers to rely on the surprise for much of their effectiveness. To achieve surprise, secrecy is required. Credible threats regarding specific means of attack or targets invite the vulnerable state to take protective actions that could blunt the threat's deterrent value. *Even if cyber weapons have the potential to cause unacceptable damage against an adversary, these are not able to offer states a credible, consistent, and 'assured' capability to do that. This deficiency significantly undermines their suitability as a deterrent tool. Instead, they are more likely to support intelligence, surveillance and reconnaissance mission or be used as a first strike weapon, preemptively, or force multipliers*.

Private Companies in Cyber Bazar

Private cyber security contractors are present all over the world. Kaspersky Lab, one of the world's leading cyber security firms, uncovered an extraordinarily sophisticated hacking operation hitting South Korea and Japan targets. It warned that "In the future, we predict the number of small, focused . . . to-hire groups to grow, specialising in hit-and-run operations, a kind of 'cyber mercenaries' of the modern world." Former director of the CIA and the NSA under President George W. Bush General Michael Hayden, stated that, "We may come to a point where defense is more actively and aggressively defined even for the private sector and what is permitted there is something that we would never let the private sector do in physical space . . . Let me really throw a bumper sticker for you: how about a digital Blackwater?[56]"

The U.S. is not alone in this configuration. France, Israel and the U.K. also rely predominantly on private contractors. In these countries, political systems, legal traditions and history distinguish strongly between the public and private spheres. The states have been under pressure to privatise and outsource its functions to save costs. The private companies offer a broad range of services. Although the contracts and services provided by the contractors for security agencies are usually classified, company and

employee websites offer some clues.

U.S. based companies are becoming increasingly sophisticated and widespread providers of cyber security products and services. Many countries are investing in home-grown cyber security markets. Several of these companies are pretty capable like, F-Secure of Finland, Kaspersky Lab of Russia and Check Point Software Technologies of Israel.

A single company might support an OCO launched by the U.S., while simultaneously providing defensive support to countries, including the target country. The consulting firm Booz Allen Hamilton is known to support the NSA of U.S. and provide cyber security services to countries in the Middle East. This scenario raises interesting questions about the choices that companies may be required to make as they consider involvement both with the U.S. government and with governments abroad.[57]

Big Guns. Private companies, including well-known defence contractors such as Lockheed Martin in the United States, BAE Systems in the U.K. or Airbus in Europe, have expanded their activities to cyber security. Countries like China do take note of this development. Northrop Grumman states on its website that its staff is "developing systems and solutions to meet the ever evolving threat and providing full-spectrum cyber operations for our customers, worldwide."[58]

Li Zheng, assistant president of the China Institute for Contemporary International Relations, a think tank affiliated with the Ministry of State Security, stated, "China is aware that the United States and other Western countries are actively using defence contractors such as Lockheed Martin, Boeing, Northrop Grumman, and Raytheon for cyber weapon development and deployment. . . The Financial Times recently said that these groups of companies had formed a 'cyber security military-industrial complex' to 'sell software to the U.S. government that can break into and degrade or destroy an enemy's computer network, as well as programmes aimed at blocking such attacks."[59]

Small but Important Players. Many innovative smaller firms have also sprung up. Examples of some of them are given below:-

ManTech of the United States. The company openly advertised "Computer Network Operations" among its capabilities, saying, "We carry out incident response, analysis and investigations, and provide information assurance and full-spectrum CNO information operations. These operations include cyber forensics and exploitation, SIGINT and cyber operations support."[60]

NICE of Israel. NICE Systems provides globally wide-ranging, state-of-the-art solutions for intelligence agencies, law-enforcement organisations, enterprises, public services and others involved in defence and security fields. NICE security solutions include products and solutions for Interception & Intelligence, covering telecom intelligence processes from monitoring, to processing, analysis and distribution of telecommunication interactions as well as incident information management solutions, capturing, managing and analyzing information for incident reconstruction, greater insight and improved response[61].

Sourgum of Israel. On July 15, 2021, the Microsoft Threat Intelligence Center (MSTIC) stated that Microsoft has been quietly tackling the threat posed to Windows operating systems by the organisation, called a "private-sector offensive actor" (PSOA). A tip provided by human rights outfit Citizen Lab led Microsoft to the PSOA, known as Sourgum.[62] This company is said to sell cyber weapons including the 'DevilsTongue' malware. Microsoft says, "The weapons disabled were being used in precision attacks targeting more than 100 victims around the world including politicians, human rights activists, journalists, academics, embassy workers, and political dissidents." Approximately half of the DevilsTongue victims are located in Palestine. However, a handful has also been traced back to countries including Israel, Iran, Spain/ Catalonia, and the U.K. According to the Citizen Lab, Sourgum is based in Israel and counts government agencies across the globe among its customers.[63,64]

Hacking Team of Italy. Italy became notorious probably when it hacked itself and saw its proprietary data spilled all over the

internet. Media reports revealed that Hacking Team was selling its offensive tools not only to law enforcement and security agencies in Europe and North America but also to countries worldwide.[65] Hacking Team develops products that allow remote access to a person's devices to monitor emails, calls, keystrokes, and location. The company's chief communications executive, Eric Rabe, has repeatedly stated that the company sells exclusively to government law enforcement or security services. The company is selling its products to the U.S. military, the company has sold them to the FBI and marketed them to hundreds of local police departments. [66,67] Other clients include the Royal Police in Thailand and the Turkish National Police and government agencies in Mexico, Singapore, South Korea and several European countries.[68]

ReVuln of Malta. It is a small company run by two Italian security researchers on the Mediterranean island of Malta. As per The New York Times, ReVuln sells zero-day vulnerabilities for industrial control systems, like those used in and power plants, water treatment facilities, oil and gas pipelines, "to countries that want to break into the computer systems of foreign adversaries." [69]

Immunity Service of U.S. Headquartered in Miami, Florida, it lists penetration testing as its "premier consulting option."[70] Founded in 2002, the "one hundred per cent American-owned business" offers its services to Fortune and Global 500 companies and "serves government departments from all over the world." It prides itself as concentrating "on purely offensive techniques," such as "developing new penetration technologies including exploits, implants, and evasion techniques. Immunity's product line remains focused on attack and penetration. Immunity delivers consulting services including penetration testing, vulnerability management, and Immunity's experts provide regular training classes."[71]

The growing demand for cyber capabilities for surveillace and coerce rivals has created entirely new types of businesses and marketplaces for state and non-state actors. Former cyber operators from multiple countries can sell their skills to the highest bidder. Left unchecked,

these actors could turn the connectivity our world relies on into a chaotic, fragmented space where states, businesses, and individuals lose trust and confidence in formal institutions.

Other Players

Cyber Militia[72]. The example of a formalised, hierarchical group that is not a private company, the Estonian Defense League's cyber unit, is being talked about as a possible model for middle-level powers. The Estonian government set it up after the 2007 DDoS attack by the Russians. The unit describes itself as "a voluntary organisation aimed at protecting Estonian cyberspace."[73] It is part of the Estonian Defense League. It counts some 15,000 members today, twice the size of the regular Estonian Defense Forces in peacetime.[74] The Estonian Defense League's function follows the classic definition of a militia: "[a] military force that is raised from the civil population to supplement a regular army in an emergency."[75] According to Estonia's Minister of Defense, Jaak Aaviksoo, the league's cyber unit "brings together specialists in cyber defence who work in the private sector as well as in different government agencies" and would function under a unified military command in wartime.[76]

False Flag Attacks. Herein, actors try to cover up their own actions by pretending to be another actor. These false flag operations are an additional challenge. The Russian cyber-espionage unit Turla hijacked the hacking infrastructure of Iranian group Oilrig. Turla used it to launch attacks in over thirty-five countries while masquerading as Iran. Russia has carried out 'false flag' operations like this in the past. Last year, U.S. intelligence uncovered Russian hackers' use of code associated with Lazarus Group, a North Korean threat actor.[77] 'Guccifer 2.0', a hacker, acted as if to be Romanian. It claimed credit for the hack of the Democratic National Committee(DNC) in 2016. Later, Guccifer 2.0 came to be known for its poor attempt to cover up the direct involvement of Russian military intelligence (General Staff Main Intelligence Directorate or GRU). When the French television station TV5 was hit with destructive malware, a group calling itself the 'Cyber Caliphate' pretending to be supporters of the Islamic State, initially claimed credit. In another case, the 'Yemen Cyber Army' came out of nowhere in the Middle East and

started defacing websites and hacking systems of the Saudi government and posting the data online. Experts disagree about the identity of the hackers, whether they are from Iran or Russia. But they are clear that the members of the Yemen Cyber Army are not from Yemen.[78]

Ultimately, proxies are here to stay. They are the pawns in the greater strategic chess game. Cyber proxies are simply the newest kids on the block

Conclusion

Cyber attacks by nation-states and supported by independent actors are becoming common. Cyber weapons are posing serious challenges for the public and private sectors alike. Key issues include attribution of cyber actions, unpredictability, potential for collateral damage, dual-use nature of cyber weapons and use of cyber weapons as force-multiplier for conventional military operations. Cyber capabilities present unique opportunities to produce a wide range of effects.

Elements that make cyber war attractive are:- [79]

- Entry costs are low. With a computer and Internet access, anyone can engage in cyberwarfare.
- Cyber operation is cheaper since it does not require large numbers of troops and weapons.
- Tools for attack are cheap and openly available on the Internet.
- Cyber operation is easy to deliver by stealth via global connectivity from anywhere.
- The proliferation of tools happens without any control.
- There are no effective technological, financial or legal hurdles to overcome against that proliferation.
- Cyber space offers the attacker anonymity. Attackers can act with

almost complete anonymity and relative impunity, at least in the short term.

- There is an advantage for the attacker who can profit from the latest and newest innovations.

- Cyber space gives unequal power to small and relatively insignificant actors operating behind false IP addresses, foreign servers and aliases.

- Cyber operation leads to the ability to disrupt the adversary rather than destroy his forces.

- Blurred traditional boundaries.

- Cyber operation enables actors to achieve political and strategic goals without the need for armed conflict.

- Cyber operation skips the battlefield. Systems that people rely upon, from banks, electric power grid, to air defence radars, all can be quickly taken over or knocked out without defeating a country's traditional defences.

- Cyber operation happens at the speed of light. It creates more risks for decision-makers, especially in a crisis.

- Potential victim of attack has to invest considerable resources to neutralising the threat.

- Vulnerabilities of countries dependent on complex, inter-connected and networked information systems increase over time, thus providing adversaries with a target rich environment.

We are beginning to see cyber capability being integrated with conventional warfare. Cyber attacks against critical infrastructures preceded Russia's invasion of Ukraine and Georgia. Future warfare will be integrated kinetic and cyber warfare. Capabilities of kinetic and cyber weapons are distinct but complementary. When applied in combination it can have a force multiplication effect. U.S. Joint Publication Cyber Space Operations (JP

3-12) of June 2018 states that "cyberspace attack capabilities, although they can be used in a stand-alone context, are generally most effective when integrated with other fires." The military is beginning to learn how, where and when to use cyber weapons. That knowledge will then allow leaders to determine if these domains could be leveraged in a complementary manner.

Cyber warfare is prone to have real physical consequences. There is no strategic reason why an attacker would limit himself to only one class of weaponry. Future wars and the conflicts that precede them will involve a mixture of kinetic weapons with cyber weaponry acting as a disrupter or force-multiplier. Many open questions remain about the integration of kinetic and cyber weapon. As leaders gain experience and expertise with cyber weapons, integrated kinetic and cyber weapon options will be strengthened. In the modern battlefield, cyber forces will be integrated into an overall battle strategy as part of a combined arms campaign. In combination, cyber weapons will be used individually and blended simultaneously with conventional kinetic weapons as force multipliers.

It must be remembered that cyber weapons are often ineffective. For both attacker and defender, it is difficult to predict. Cyber weapons often achieve things other than their intended purpose. Deception provides abilities to defenders to reroute or mitigate incoming threats. Attackers may not be able to comprehend this. Strategic calculation for attackers thus becomes considerably more complex. Over-reliance by strategists and scholars on such imprecise terminology has significant risks for misinterpretation and premature prescription.

Cyber weapons may not produce the physical destruction and loss of life traditionally linked to kinetic weapons. Nevertheless, they have significant impacts. In 2018 U.S. Cyber Command acknowledged this strategic significance of below-the-threshold engagements in cyber space required to compete successfully.

References:

1. U.S. DEP'T OF DEFENSE, DEPARTMENT OF DEFENSE CYBER POLICY REPORT, 2011.

2. Przemysław Roguski, An Inspection Regime for Cyber Weapons: A Challenge Too Far? Cambridge University Press, March 01, 2021 available at: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/an-inspection-regime-for-cyber-weapons-a-challenge-too-far/0FD64925A8CA9DDBCB7AF05F6CBEAB2D#fn7

3. Dr. Chase Cunningham, Cyber Warfare – Truth, Tactics, and Strategies, Packt Publishing, 2020.

4. Clay Wilson, Cyber weapons: 4 defining characteristics. June 04, 2015 available at: HTTPS://GCN.COM/ARTICLES/2015/06/04/CYBER-WEAPON.ASPX

5. 11 NICOLAS FALLIERE ET AL., W32.STUXNET DOSSIER, SYMANTEC-SECURITY RESPONSE (2011).

6. Przemysław Roguski, An Inspection Regime for Cyber Weapons: A Challenge Too Far? Cambridge University Press, March 01, 2021 available at: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/an-inspection-regime-for-cyber-weapons-a-challenge-too-far/0FD64925A8CA9DDBCB7AF05F6CBEAB2D#fn11

7. Jake Williams, What You Need to Know About the SolarWinds Supply-Chain Attack, SANS BLOG (Dec. 15 2020).

8. David E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, N.Y. TIMES, June 1, 2012.

9. M. Carr, US power and the internet in international relations the irony of the information age, Basingstoke: Palgrave Macmillan, 2016, p.37.

10. Eric Rosenbach, Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks, Testimony Before the Senate Foreign Relations Committee, Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, June 12, 2017.

11. Steven M. Bellovin, Susan Landau, and Herbert S. Lin, Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications, Journal of Cybersecurity 3, no. 1, March 2017, pp. 59–68.

12. Julian E. Barnes and Thomas GibbonsNeff, U.S. Carried Out Cyberattacks on Iran, New York Times, June 22, 2019.

13. Task Force on Cyber as a Strategic Capability: Executive Summary, Washington, DC: Department of Defense, June 2018.

14. Nicola Bates, Comparing Cyber Weapons to Traditional Weapons Through the Lens of Business Strategy Frameworks, Information Security Group , Royal Holloway, University of London.

15. L. Kello, The Meaning of the Cyber Revolution: Perils to Theory and Statecraft, International Security, Vol. 38, 2013, pp. 7-40.

16. EU Cyber Direct, The application of existing international law in cyberspace: state practice and key concepts, July 9, 2018 available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/programme_international%20law%20in%20cyberspace_07.07.2018.pdf

17. Department of Defense, Office of General Counsel, "Weapons," in Law of War Manual (2015), p. 340.

18. M. Schmitt and NATO Cooperative Cyber Defence Centre of Excellence. Tallinn manual on the international law applicable to cyber warfare : Prepared by the international group of experts at the invitation of the NATO Cooperative, New York : Cambridge University Press, 2013.

19. M. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017.

20. M. L. Gross, D. Canetti and D. R. Vashdi, "Its Effects on Psychological Well-Being, Public Confidence, and Political Attitudes," in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, H. Lin and A. Zegart, Eds. Washington, D.C.: Brookings Institution Press, 2018, pp. 239."

21. L. Kello, The Virtual Weapon and International Order, Hampshire: Yale University Press, 2018.

22. Sue Halpern**,** How Cyber Weapons Are Changing the Landscape of Modern Warfare, The New Yorker available at : https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare

23. K. Zetter, How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, Wired, July 11, 2011 available at: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

24. The SolarWinds Cyber-Attack: What You Need to Know, Center for Internet Security, March 15, 2021 available at: https://www.cisecurity.org/solarwinds/

25. SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president, Reuters, February 15, 2021 available at: https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idINKBN2AF03R

26. Isabella Jibilian, The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal, Business Insider India, April 15, 2021 available at: https://www.businessinsider.in/tech/news/heres-a-simple-explanation-of-how-the-massive-solarwinds-hack-happened-and-why-its-such-a-big-deal/articleshow/79945993.cms

27. Dina Temple-Raston, A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack, NPR, April 16, 2021 available at: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

28. Kate Conger and Sheera Frenkel, Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China, The New York Times, March 6, 2021 available at: https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html

29. HAFNIUM targeting Exchange Servers with 0-day exploits, Microsoft, March 2, 2021 available at: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

30. David Smith, US condemns China for 'malicious' cyberattacks, including Microsoft hack, The Guardian, July 20, 2021 available at: https://www.theguardian.com/technology/2021/jul/19/microsoft-exchange-hack-us-biden-administration-china

31. The CIA Hacking Group (APT-C-39) Conducts Cyber-Espionage Operation on China's Critical Industries for 11 Years, available at: https://blogs.360.cn/post/APT-C-39_CIA_EN.html

32. Meat giant JBS pays $11m in ransom to resolve cyber-attack, BBC News, June 10, 2021 available at: https://www.bbc.com/news/business-57423008

33. A 'Colossal' Ransomware Attack Hits Hundreds Of U.S. Companies, A Security Firm Says, NPR, July 3, 2021 available at: https://www.npr.org/2021/07/03/1012849198/ransomware-cyber-attack-revil-attack-huntress-labs

34. Ellen Nakashima, Pressure grows on Biden to curb ransomware attacks, The Washington Post, July 7, 2021 available at: https://www.washingtonpost.com/national-security/ransomware-biden-russia/2021/07/06/ff52a9de-de72-11eb-b507-697762d090dd_story.html

35. Mike Chapple, Ransomware is a national security risk. It's time to treat it like one, CNN Business Perspectives, June 10, 2021 available at: https://edition.cnn.com/2021/06/10/perspectives/ransomware-attacks-national-security/index.html

36. Jenny Jun, Could Ransomware Become a Geopolitical Weapon? Game Theory Says Yes, July 08, 2021 available at: https://www.politico.com/news/magazine/2021/07/08/ransomware-game-theory-geopolitics-cyber-attack-498625

37. Dina Temple-Raston, A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack, NPR, April 16, 2021 available at: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

38. United States Government Launches First One-Stop Ransomware Resource at StopRansomware.gov, Homeland Security, July 14, 2021 available at: https://www.dhs.gov/news/2021/07/14/united-states-government-launches-first-one-stop-ransomware-resource

39. Jenny Jun, Opinion | Could Ransomware Become a Geopolitical Weapon? Game Theory Says Yes. POLITICO, July 08, 2021 available at: https://www.politico.com/news/magazine/2021/07/08/ransomware-game-theory-geopolitics-cyber-attack-498625

40. Hackers Attack Every 39 Seconds, February 10, 2017 available at: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds

41. Forbes, Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits, Forbes, March 23, 2012 available at: http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

42. Commodification of Cyber Capabilities: A Grand Cyber Arms Bazar, Public Private Analytic Excange Program, November,2019 available at: https://nsiteam.com/social/wp-content/uploads/2019/11/191119-AEP_Commodification-of-Cyber-Capabilities-Paper.pdf

43. APT trends report Q2 2019, GReAT, August 1, 2019 available at: https://securelist.com/apt-trends-report-q2-2019/91897/

44. For example, the Russian-backed group Sandworm used a destructive piece of malware called NotPetya to attack Ukraine and through a widely used tax software. Although targeting was regional, NotPetya inadvertently spread on a global scale, crippling international corporations such as Maersk and Merck as well as shipping, construction, and agriculture industries.

45. Justin Sherman, Digital authoritarianism and the threat to global democracy, Bulletin of the Atomic Scientists, July 25, 2019 available at: https://thebulletin.org/2019/07/digital-authoritarianism-and-the-threat-to-global-democracy/

46. Ibid

47. Department of Defense, Defense Science Board. 2013. Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. Washington, DC: The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, available at: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

48. In addition to DarkMatter, NSO Group and FinFisher several other firms are competing in this space: Verint, Interionet, Gamma Group, Intellexa, Black Cube, CyberPoint International, Senpai Technologies, Al-Thuraya Consultancy & Research, Omniscope Limited, Q_Cyber Technologies, and SecureTech.

49. Marczak, Bill, John-Scott Railton, Adam Senft, Brene Poetranto, Sarah McKune, Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation, Citizen Labs, October 15, 2015 available at: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/#2

50. Mazzetti, Mark, Adam Goldman, Ronen Bergman and Nicole Perlroth, A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments, New York Times, March 21, 2019 available at: https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html

51. Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities, Committee on Armed Services House of Representatives one hundred fifteenth Congress First Session Hearing held march 1, 2017.

52. Michael V. Hayden, Playing the Edge, American Intelligence in the Age of Terror, New York: Penguin Press, 2016.

53. Andy Greenberg, This Map Shows the Global Spread of Zero-Day Hacking Techniques, Wired, available at: https://www.wired.com/story/zero-day-hacking-map-countries/

54. James Lewis, The Korean Cyber Attacks and Their Implications for Cyber Conflict, Center for Strategic and International Studies, October 23, 2009

available at: http://csis.org/publication/korean-cyber-attacks-and-their-implicationscyber-

55. John Markoff and Thom Shanker, Halted '03 Plan Illustrates US Fear of Cyber Risk, The New York Times, August 1, 2009 available at: http://www.nytimes.com

56. Andrew Nusca, Hayden: 'Digital Blackwater' May Be Necessary for Private Sector to Fight Cyber Threats, Between the Lines (blog), ZDNet, August 1, 2011 available at: www.zdnet.com/blog/btl/hayden-digital-blackwater-may-be-necessary-for- private-sector-to-fight-cyber-threats/53639

57. Tim Shorrock ,Spies for Hire: The Secret World of Intelligence Outsourcing , Simon & Schuster, 6 May 2008 available at: https://www.scribd.com/book/224446965/Spies-for-Hire-The-Secret-World-of-Intelligence-Outsourcing

58. "Cyberpatriots," Northrop Grumman available at: https://www.northropgrumman.com/Careers/%20StudentsAndNewGrads/Pages/Cyberpatriot.aspx

59. Li Zhang, A Chinese Perspective on Cyber War, International Review of the Red Cross 94: 805, 2012 available at: http://e-brief.icrc.org/wp-content/uploads/2016/09/43.-A-Chinese-perspective-on-cyber-war.pdf

60. "Capabilities," Cybersecurity, ManTech International Corporation available at: https://www.mantech.com/capabilities

61. Cyber Tech, Events around the world available at: https://www.israeldefense.co.il/en/company/nice-systems

62. Cristin Goodwin, Fighting cyberweapons built by private businesses, Microsoft, Jul 15, 2021 available at: https://blogs.microsoft.com/on-the-issues/2021/07/15/cyberweapons-cybersecurity-sourgum-malware/

63. Bill Marczak et al., Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus, Citizen Lab, July 15, 2021 available at: https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

64. Charlie Osborne, Microsoft points the finger at Israeli spyware seller for DevilsTongue attacks, ZDNet, July 16, 2021 available at: https://www.zdnet.com/article/microsoft-points-the-finger-at-israeli-private-exploit-seller-for-devilstongue-malware-attacks/

65. On WikiLeaks, Business Standard, July 10, 2015 available at: https://www.business-standard.com/article/current-affairs/india-s-spy-agencies-explored-

sypware-from-hacking-team-leaked-mails-on-wikileaks-115071001148_1.html

66. Ellen Nakashima and Ashkan Soltani, "Italian Spyware Firm Relies on U.S. Internet Servers," Washington Post, March 3, 2014 available at: www.washingtonpost.com/ world/national-security/italian-spyware-firm, Cora Currier and Morgan Marquis-Boire, "Leaked Documents Show FBI, DEA and U.S. Army Buying Italian Spyware," The Intercept, July 6, 2015 available at: https://theintercept.com/2015/07/06/hacking-team-spyware-fbi/

67. Shawn Musgrave, Hacking Team Had Ties to Local Police Departments Across the US, Motherboard, Vice, July 24, 2015 available at: http://motherboard.vice .com/read/hacking-team-had-ties-to-local-police-departments-across-the-us

68. Bill Marczak, What We Know About the South Korea NIS's Use of Hacking Team's RCS, Citizen Lab, August 9, 2015 available at: https://citizenlab.org/2015/08/what- we-know-about-the-south-korea-niss-use-of-hacking-teams-rcs/-relies-on-us-internet-servers/2014/ 03/03/25f94f12-9f00-11e3-b8d8-94577ff66b28_story.html

69. Nicole Perlroth and David E. Sanger, Nations Buying as Hackers Sell Flaws in Computer Code, New York Times, July 13, 2013 available at: www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html

70. Penetration Testing, Immunity Inc. available at: https://immunityinc.com/services/penetration-testing.html

71. Who We Are, Immunity Inc. available at: www.immunitysec.com/company/

72. Ariel Ahram, Proxy Warriors: The Rise and Fall of State-Sponsored Militias, Stanford University Press, 2011 available at: https://www.sup.org/books/title/?id=18167

73. Estonian Defence Forces available at: www.mil.ee/en/ defence-forces

74. Estonian Defence League's Cyber Unit, Estonian Defence League available at: www.kaitseliit.ee/en/cyber-unit

75. "militia," Oxford Dictionaries available at: https://en.oxforddictionaries.com/definition/ militia

76. Tom Gjelten, Volunteer Cyber Army Emerges in Estonia, NPR, January 4, 2011 available at: https://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation

77. Nicole Perlroth, Report Says Cyberattacks Originated Inside Iran, New York Times, December 2, 2014 available at: www.nytimes.com/2014/12/03/world/middleeast/ report-says-cyberattacks-originated-inside-iran.htm

78. Sheera Frenkel, Meet the Mysterious New Hacker Army Freaking Out the Middle East, Buzz Feed, June 23, 2015 available at: www.buzzfeed.com/sheerafrenkel/who-is-the-yemen-cyber-army

79. Fred Schreier, On Cyberwarfare, DCAF HORIZON WORKING PAPER No. 7, 2015 available at: https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organisation to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelise fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its inception, VIF has pursued quality research and scholarship and made efforts to highlight issues in governance, and strengthen national security. This is being actualised through numerous activities like seminars, round tables, interactive dialogues, Vimarsh (public discourse), conferences and briefings. The publications of VIF form lasting deliverables of VIF's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

VIVEKANANDA INTERNATIONAL FOUNDATION
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Phone: +91-11-24121764, 24106698
Email: info@vifindia.org,
Website: https://www.vifindia.org
Follow us on twitter@vifindia