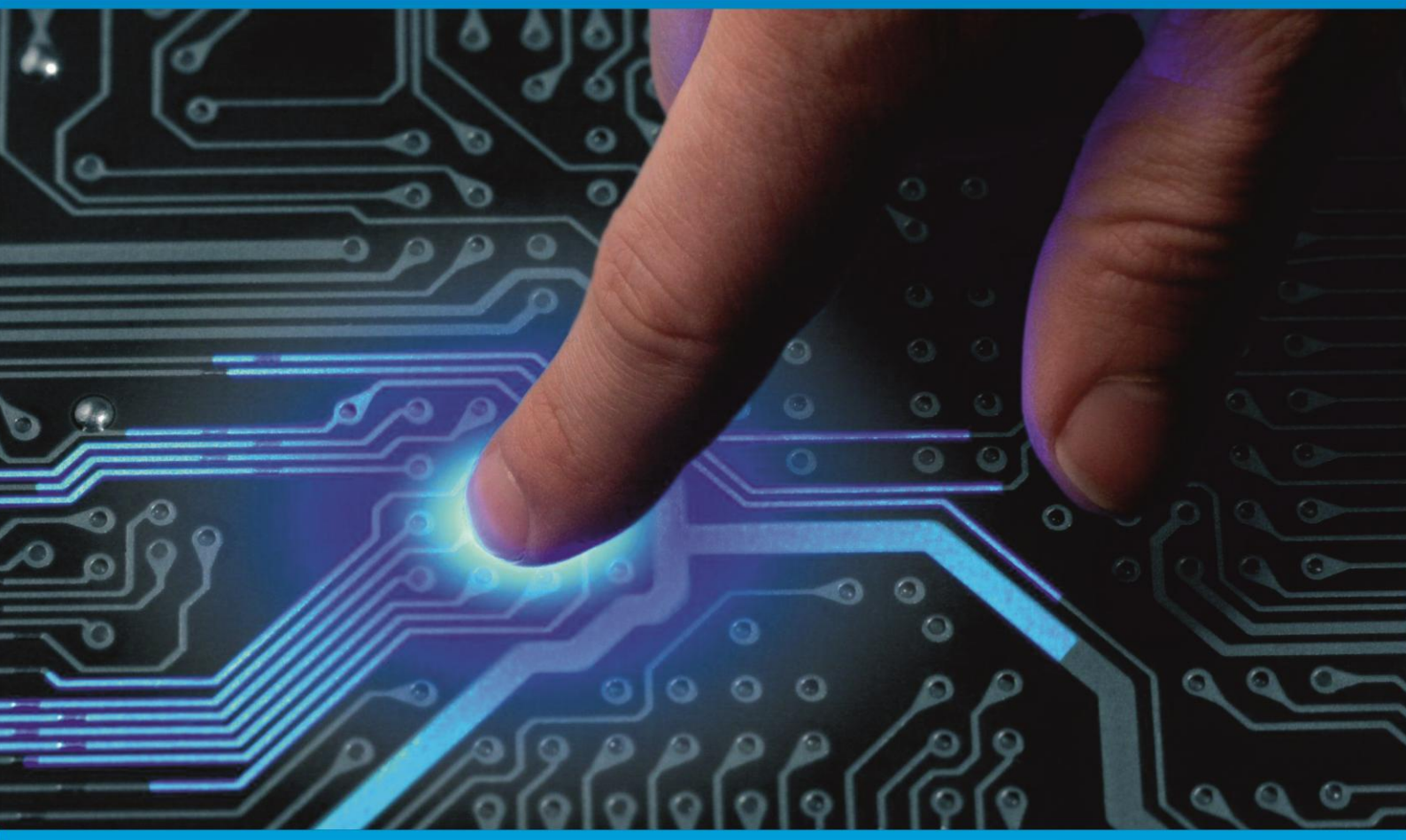
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905035 |

A Systematic Review Multiple Scenarios of Cyber Warfare and Its Impact

Shashwat Simon[1], Shaswat Singh [2], Rajeshwari Gundla[3]

U.G Student, School of Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India [1, 2]

Assistant Professor, School of Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India [3]

ABSTRACT: The topic of cyber warfare is a vast one, with numerous sub topics receiving attention from the research community. First we examine the foremost basic question ie what is cyber warfare, comparing existing definitions to seek out footing or disagreements. We discover that there's no widely adopted definition which the terms cyber war and cyber warfare aren't tolerably differentiated. To address these issues, we present a definition model to assist define both cyberwarfare and cyber war. The paper describes eight research challenges within the cyber warfare domain and analyze contemporary work administered in each one of it. We can conclude it by making some suggestions on, how the sector can be best progressed by some future efforts.

KEYWORDS: Cyber War, Cyber Warfare

I. INTRODUCTION

Cyberwarfare can be a powerful weapon in propaganda, political conflicts and espionage. It's difficult to detect it priory, it is only recognized after significant damage has been done. Gaining offensive potential on the cyber battleground figures noticeable in the countries national strategies and is explicitly stated in the doctrines of majority, including Russia, India, U.S, and the China. It is understood that they are laying the foundation for potential cyber conflicts by exploiting the networks of nemesis and allies alike. Cyberwarfare escapade are drastically increasing not only among the nation and states but also among the political/social, terrorists and transnational organizations. [1]
A crucial example of cyberwarfare was the 1999 targeting of the U.S. government Sites by suspected Chinese hackers in the after effect of the fortuitous, as the officially reported, U.S. attacking Chinese embassy in Belgrade in 1999.
Cyberwarfare has been perceiving mostly as nuisance attacks (such as Dos and Web-site defacement, or denial-of-service), with only irregular occurrence of surveillance and infrastructure probes. In few and far between cases, these attacks have resulted large-scale failure of the public Internet though have not resulted in loss of life, destruction of property or large-scale injury.

Future attacks could involve destruction of information and communications systems and infrastructure and psychological operations. The cyberattack against Georgia in 2008 and Estonia in 2007 hinted at the potential of cyberwarfare. The prospective crippling impact to critical national infrastructure has established the role of cyberwarfare in modern conflicts. The techniques & tools for attacking in cyberwarfare are the same as in cybercrime. However, the delinquent impulses differ from the political objectives of cyberwarfare to the significant financial incentives motivating much of today's cybercrime. In addition, scale, intention, and consequences can be much more severe for cyberwarfare. The publicly reported losses incurred due to cybercrime in the U.S. have escalated steadily, totalling to approx. $560 million in 2009, according to the U.S. Department of Homeland Security. Such losses are due in part to increased sophistication

II. PRINCIPLES OF CYBERWARFARE

Cyberwarfare is different from traditional kinetic warfare and thus requires a review of basic warfare principles to differentiate it from armed conflict in the traditional sense. [2]

To present our cyberwarfare principles, we must define our terms. Dan Kuehl has defined cyberspace as "a functional area where peculiar and unique characters are framed by the use of electronics and the electromagnetic spectrum to pool, manufacture, exchange, alter and exploit information through interconnected information communication

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905035 |

technology (ICT) based on systems and their correlated infrastructures." This coincides with our actual description of the cyber world as any virtual reality accommodated in a troupe of nodes and networks. Many cyber worlds exist, but the one most suitable to present cyberwarfare discussions is the Internet [2]. Cyberwarfare is a fusion of computer network attack & defence and special technical operations. We define kinetic warfare as warfare practiced in the land, sea, air, and space domains. All present militaries' equipment's such as ships, tanks, planes, and soldiers are kinetic warfare's protagonists.

1. Lack of Physical Limitations

Physical limitations of distance and space doesn't apply in cyber world. In cyber world, physical distance is neither a barrier nor a facilitator in conducting attacks. A cyberattack can be accomplished with equal efficiency from the other part of the world as from the room next door. In kinetic warfare, attacks are implemented by physical articles that must travel to an extent. These attacks are restricted to those who have the technology to make that object to travel that distance.

In our red-teaming work, we've mapped out, developed, and carry out attacks that turn out in the room next door, diverse locations around the globe, and all points in between. The emerging and extensive use of wireless networks have joined the RF side of the physical dimensional attacker in the parking lot can be as dangerous as one in the server room.

Attacks can use mediator systems, networks, and even human actors to prevent attribution by the protectors. Obtaining relevant mass in the kinetic world has physical drawbacks. The formation of mass in the cyber world doesn't seem to have these drawbacks [11,3]. An attacker can create several clones of a cyber-weapon with almost no expense of time or matter; primarily its extensive and unconstrained as a "matter" element of warfare [12,9].

2. Kinetic Effects

Cyberwarfare should have kinetic world consequence. It is nonsensicalunless ithas an effects on someone or something in the physical world. Attackers can attack organizations, institutions in the cyberspace as much as they want, but unless something reflects in the real world as an outcome, they might as well be playing Core Wars. Cyberwarfare can have straight affect objects in the real world, such as the opening of a dam spill gate or lockdown of an electrical substation. Cyberwarfare in its most minute form can influence the minds of decision makers. The formeris comparable to kinetic warfare, the end is more purely a form of information warfare, in which attacker's current adversary with intelligence that leads to bad selection.

Examples of physical world sequel abound the Aurora exposition by Idaho National Laboratories showed that cyber manipulation of an electrical power grid can cause instruments miscarriage [13,8]. In the course of our red-teaming, we uncovered the prospect of attacks that would open dam floodgates and cause railroad calamity. Earlier attacks have overblown both tactical and strategic decision makers. Attackers can deceive strategic decisionmakers about the placement and size of rival and friendly forces. At an operative level, we red-teamed a logistics system to influence the arrival time and volume of supplies and reinforcements to cause bad decisions, such as striking with inadequate ammunition and detaining attack through panic of lack of supplies.

In addition, strategic decision makers might be hoax by attributing operations to other Nations or groups than the actual attacker. We co-developed a framework for a cyber-defence seminar that focused on an opponent venturing to whip up war between two nations via cyberwarfare. The participants playing the part of the government leaders could not discover the actual contender.

3. Stealth

People can take active steps to hide in the cyber world, but everything we do is visible. The query is whether someone is inspecting at the right place within the right time.

The cyber world is an unnatural one, created by human beings by utilizing software and hardware. Any actions combatants take in that world require data movement or manipulation—some bit in some data stream is changed to reflect their presence and actions. This is good news for defenders, but it's only useful if the defenders are looking.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905035 |

Since writing our previous article, intrusion detection and prevention and attack correlation technology have improved—but the attacker can still use stealth to hide in the bits.

Hiding in the cyber world is analogous to using camouflage in the physical world. Physical world combatants can modify their sensor footprint using stealth technology. In cyber world, contender cannot take steps identical to engrossing radar energy or cooling infrared signatures. Rather, cyberwarfare supporter must try to hide proofs in the existing data streams. Sensors looking for cyberattacks must distinguish between bits that are an attacker's artefact and the overwhelming majority that are normal activity. Using normal activity to conduct an attack complicates this. For instance, signaturebased intrusion detection systems cannot distinguish between a normal database user and an adversary manipulating the database as that user.

The fact that some data, such as network packets, is ephemeral means that defenders must capture it to a more persistent medium. However, such global data collection creates its own problems with data analysis—the "needle in the haystack" problem.

4. Mutability and Inconsistency

There are no immutable laws of physics in the cyber world except those that require a physical world action to change. Cyberspace is sufficiently mutable so
it is neither consistent nor reliable. This principle was originally two separate principles, but because they're so interrelated, we combined them.

First, we address the inconsistency of cyberspace. In the physical world, we can expect that a bullet will act in a certain way when fired—we can predict the bullet's path with ballistics. Each time a shooter triggers a bullet, it will act equivalently, withina contrast due to slight physical causes. In the cyber world, nothing can be taken for granted in this way. The cyber world, as anartificial construct built by humans, is imperfect. It can and does change in ways that seem chaotic. Software and hardware fail programs run faster than expected, these and a thousand other mutants cause unpredictability [14,5].

In cyberwarfare, this inconsistency translates to attacks that do not always behave the same way, environments that change midattack, and fluctuations in attack performance. The only aspects of the cyber world that don't change are those that require a physical world modification. For example, a software's performance cannot exceed a computer's processing powers capability until unless a real world person migrates to an accelerated processor. Communications bandwidth is limited by the telecommunications infrastructure and can only be changed by changing that infrastructure.

An example of real world experience that supports this occurs during sniffing of packets. We frequently see one set of connections and packet streams during discovery only to find a different set when we attempt our attack.

Another fact of cyberspace's artificial character stick is that it is unreliable. Neither hardware nor software will everytime work as anticipated in cyberspace. This is true more of software, but we've seen hardware inconsistencies, usually because of heat or power loads.

One effect of this principle is that we can never be certain that a particular step in an attack will work. We plan attacks using diagrams that show the change in a system's state from the initial adversary access to the point of reaching the goal. Each path through the diagram is an attack scenario, and the set of attack scenarios that a particular attacker can achieve is a scenario set. Attack scenarios comprise individual attack steps—information gathering, setups, and dastardly deeds. Each attack step has an uncertainty factor. In one engagement, we had carefully collected local privilege escalation exploits to use after we gained remote user access to a knownversion of Solaris. However, we were frustrated to find that none of the exploits worked, despite being aimed at the correct version of Solaris. Because this was a reteaming engagement in cooperation with the defenders, we were talking to the defenders. One of the target network's administrators informed us that a variant of an exploit that was supposedly fixed two versions earlier worked quite well. In another exercise, we conducted system scans with multiple tools, then spent days trying to understand why the results were so different. This effect was even more pronounced when wescanned a global enterprise's networks for exposed services. Three separate scans found different quantities of systems—120,000 systems on one,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905035 |

160,000 on another, and 140,000 on a third. The changes were due to physical world changes laptops disconnected, systems turned on or off, network connectivity lost.

Another effect of the lack of consistency and reliability is that attacks we do not expectto succeed frequently do. In one exercise, we believed that the defenders had successfully hidden unencrypted password traffic in a VPN. Much to our surprise, they had left one service outside the VPN, which provided us with the necessary password to log in as the database administrator. That particular exercise taught us that risk calculation must include the potential benefit to the adversary as well as attack metrics, such as difficulty and probability of success.

5. Identity and Privileges

Some institutes in cyber world has the accessibility, ability, or authority to carry out any measures an attacker hankering to carry out. The attacker's aim is to presume the identification of that entity, in some fashion.

Again, because the cyber world is a truly artificial construct, it's put up and administered by humans and their tools. There is no part of the cyber world that is not administered by a person or that person's cyber entity. At times the entity with the authority, ability, or accessibility is an icon. At times the human assigns the control to a software element. But there's always something or someone who can do what the cyber combatant wants to do. Majority of the steps in any cyberwarfare attacks are wilful to simply presume the identity of the institution that can carry out the desired action.

A finest example is the Unix root exploit. When attackers carry out a root exploit, they're striving to presume the identity of a Unix system root super user. In our exercises, we used root exploits as steps in attacks that involved changing the target systems' configuration or software.

Though, the root exploit is not the only example, or even the most common. During the course of many exercises, we located and stole the identities of standard users, database administrators, system programs (such as Unix daemons and Windows services), and developers. In every case, we first found out who or what could perform the action, and then we worked to assume that identity.

6. Dual Use

Cyberwarfare tools are always dual use, whereas the tools of kinetic warfare are more single purpose, primarily used for one purpose of offense,defence, or sensing. Weapons are used to attack, armour is used to defend, and sensors are used to detect the enemy. In kinetic warfare, defenders do not test theirdefences by shooting their own troops or equipment. Commanders of an ambushing unit might use night vision gear to look at their own troops from the enemy's viewpoint to ensure the ambush's success. This use of sensors is both offensive and defensive, but this is an exception to the rule.

Attackers and defenders in cyberwarfare use the same tools. Attackers use vulnerability scanners to look for exploit opportunities as part of an attack. Defenders use the same vulnerability scanners to look for weaknesses in their own systems. Packet capture devices emerged since the network administrators had analyse the packet traffic to diagnose and troubleshoot the network issues. Attackers use packet capture for discovery. Attackers collect exploits to use against their targets. Defenders collect exploits to test their own systems, because mission or business requirements might prevent patching and because those systems can regain vulnerabilities from poor vendor upgrades.

Kinetic weapons are used against representative samples of physical world defences and systems to study their effects, but not against actual defences or systems because of the costing both money and timing of reconstituting affected systems. We don't normally bomb our own missile silos, tanks, airfields, and ships. However, cyber weapons are routinely used against actual defences and systems (as with penetration testing) with the belief that these systems can be rebuilt for almost no cost.

7. Infrastructure Control

Both defenders and attackers control a very small part of the cyberspace they use. Whoever controls a part of cyberspace that the opponent uses can control the opponent, thus the most recent trend is toward testing one's own networks by attacking them pre-emptively. Normally, the limitation of the controlled cyberspace is the real physical

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905035 |

circumference, scarcely does a cyber-group control anything beyond its interface with the communications infrastructure. After the Persian Gulf War, open literature hypothesized that the DoD directly controls only 10 percent of the communications infrastructure used for DoD traffic, with the remaining fraction under commercial providers' control. This means that neither the attacker nor defender controls 90 percent of the infrastructure used in the course of its activities. Thus, both parties are vulnerable to attacks on third party infrastructure. If one or the other can gain control of part of that infrastructure, that party gains a significant advantage.

An example of this quest for control is Domain Name System (DNS) attacks. DNS provides the glue on which applications rely to find each other. Over the years, many publicly disclosed DNS attacks have occurred, which we used in our simulation exercises. Once we gained control of a DNS, the target applications found other applications only if we allowed it. We used this type of attack to bypass an early implementation of Internet Protocol Security (IPsec) during an exercise in June 2000.

Another example of this quest for control is the use of Border Gateway Protocol spoofing to control routes to Georgian government websites during the Russian cyberwar with Georgia[14,4].Georgian sites were inaccessible because traffic to them was routed through autonomous systems purported to be controlled by the Russian Business Network.

8. Information as Operational Environment

The terrain, the weather, the enemy—every part of warfare's operational environment is information.
If warriors perform Joint Information Preparation of the Operational Environment (JIPOE) for kinetic warfare, they collect information about each of these factors that represents the underlying physical reality. The collection requires sensors that transform the physical reality into information. In cyberwarfare, it's the information itself that constitutes JIPOE. The communication connections, computer network maps, personnel rosters, websites, links, emails, posing, and every other aspect of the target is already information in cyberspacethere's no conversion from physical measurements to information.

III. CONCLUSION

Cyberwarfare is different from conventional, kinetic warfare. Like its parent, information warfare, many of its characteristics depend on human frailties. One of the elementary variance among cyberwarfare and kinetic warfare is the nature of their environs. Kineticwarfare takes place in the real world, administered by physical laws that we areaware and understand with respect to warfare. Cyberwarfare takes place in an artificial, manmade world that's constantly changing. Cyberwarfare can use some principles of kinetic warfare, but others have little or no meaning in cyberspace. For these reasons, the fundamentals of cyberwarfare are eventually, non-identical from those of kinetic warfare. Using the principles of cyberwarfare should lead to success in cyberwarfare. We believe we have some of the principles right, but by no means do we believe we are completely correct. This is the first step in the process of developing the real principles; years of experience will show what will win and what will lose. We do not claim to be the Sun Tzu or Clausewitz of cyberwarfare—we are the unknown cavemen who first chipped rocks into spearheads and knives and fought over herds of wild animals.

REFERENCES

1. Sanjay Goal. 2011. Cyberwarfare: connecting the dots in cyber intelligence. *Common. ACM* 54, 8 (August 2011), 132–140. DOI:https://doi.org/10.1145/1978542.1978569
2. R.C. Parks and D.P. Duggan, "Principles of Cyberwarfa re," Proc. 2001 IEEE Workshop on Information Assurance and Security, IEEE CS Press, 2001; www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA424310.
3. D. Kuelh, "From Cyberspace to Cyber power," Cyber power and National Security, F.D. Kramer, S.H. Starr, and L. Wentz, eds., Potomac Books, 2009.
4. US Dept. of Defence Joint Publication 3-13, "Joint Doctrine for Information Operations," 9 Oct. 1998; www.c4i.org/jp3_13.pdf.
5. T. Tzu, The Art of Strategy, Doubleday, 1988.
6. C. von Clausewitz, VomKriege (O n War), CreateSpace, 2009.
7. B.H. LiddelHart, Strategy, 2nd ed., Plume, 1991.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905035 |

8. US Dept. of Defence Joint Publication 1, "Doctrine for the Armed Forces of the United States," 14 May 2007; www.dtic.mil/doctrine/new_pubs/jp1.pdf.

9. G. Schudel, B. Wood, and R. Parks, "ModelingBehavior of the Cyber Terrorist," Nat'l Security Forum Int'l Cooperation to Combat Cyber Crime and Terrorism, Hoover Inst. Press, 1999.
10. R. Duggan, "Insider Adversary Model Briefing," DARPA IASET Insider Workshop, DA R PA, 2000.
11. S.M. Convertino, L.A. DeMatiei, and T.M. Knierim, "Flying and Fighting in Cyberspace," July 2007; www.au.a f.mi l /au/awc/awcg ate/m a x wel l /mp4 0. pd f.
12. J.E. Dunn, "WikileaksDDoS Tool Downloads Grow Rapidly," Network World, 10 Dec. 2010; www.networkworld.com/news/2010/121010-wikileaks-ddos-tool-downloads-grow.html.
13. J. Meserve, "Sources: Stage Cyber Attack Reveals Vulnerability in Power Grid," CNN, 26 Sept. 2007; http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US.
14. G.J. Rattray, Strategic Warfare in Cyberspace, MIT Press, 2001.
15. "Georgia Cyberwarfare," Russian Business Network, 9 Aug. 2008; http://rbnexploit.blogspot.com/2008/08/rbngeorgia-cyberwarfare.html

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details