



Vivekananda  
International  
Foundation

VIF Brief | May 2022

# **Decoding Russia's 'Missing' Cyberwar Amid War in Ukraine**

Maj Gen PK Mallick, VSM (Retd)

© Vivekananda International Foundation

Published in 2022 by

Vivekananda International Foundation

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

Tel: 011-24121764 | Fax: 011-66173415

E-mail: [info@vifindia.org](mailto:info@vifindia.org)

Website: [www.vifindia.org](http://www.vifindia.org)

Follow us on

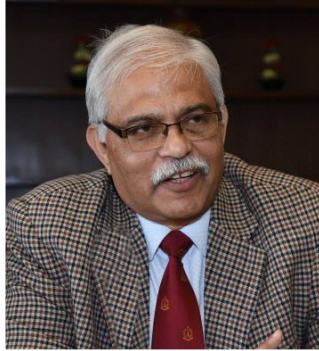
Twitter | [@vifindia](https://twitter.com/vifindia)

Facebook | [/vifindia](https://www.facebook.com/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 The author certifies that the article/paper is original in content, unpublished and it has not been submitted for publication/web upload elsewhere, and that the facts and figures quoted are duly referenced, as needed, and are believed to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.

All Rights Reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying, recording or otherwise without the prior permission of the publisher.



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 website on national security issues @ <https://www.strategicstudyindia.com>.

# **Decoding Russia's 'Missing' Cyberwar Amid War in Ukraine**

Predicting future war is difficult. It was envisaged that cyber operations would take a very big lead in the ongoing conflict in Ukraine. Before Russia started invasion in Ukraine on February 24, experts predicted cyber attacks to play a crucial role in the conflict. Despite Russia's strong cyber capabilities, however, there has been relatively little visible action against Ukrainian systems via cyberattacks. The Ukrainian Army's command-and-control communications systems is working satisfactorily. Russia has not used cyber operations as an integral part of its military campaign to facilitate the advance of ground or air forces. The reasons for this underuse of Russia's sophisticated cyber capabilities so far in the conflict are unclear.

Probably Russia has carried out fewer and less-severe cyberattacks against Ukraine than it could have. We do not know the extent of what has happened on the cyber battlefield in this conflict. Russia may be withholding cyber weapons for use against the Western powers especially the U.S. at a later stage of the war. It is unlikely that everything the Russians may be doing has been made public. The factual details of the cyber warfare part of the Russian invasion of Ukraine may come out until after the conflict ends.

An analysis of Cyber Warfare on the Russia-Ukraine conflict is carried out based on open source information.

**Russia's Standing in Cyber World.** Belfer Center for Science and International Affairs, Harvard Kennedy School, has categorised Russia fourth behind U.S., China and U.K in its National Cyber Power Index in 2020<sup>1</sup>. The recent International Institute for Strategic Studies (IISS) Report on Cyber Capabilities and National Power<sup>2</sup> has assessed U.S. as a first tier cyber power. Russia along with Australia, Canada, China, France, Israel and the U.K. are considered as Tier two power.



Source : <https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power>

As per the Global Cybersecurity Index (GCI), an International Telecommunication Union (ITU) initiative, Russia was ranked in cyber security, fifth out of 175 countries, in the International Telecommunication Union's 2020 Report<sup>3</sup>.

**Russia's Demonstrated Cyber Warfare Capabilities.** Russia has demonstrated its cyber warfare capabilities many times *e.g.* Estonia in Apr – May 2007 and Georgia in 2008. First time in the history of warfare a co-ordinated cyberspace domain attack synchronised with significant combat actions in the other warfighting domains of ground, air and sea took place in Georgia.

In Ukraine, Russia's 2014 annexation of Crimea included cyber operations simultaneously with kinetic ones. Two Attacks on Ukraine's Power Grid were carried out in 2015 and 2016. In June 2017, the Russian military intelligence service launched cyber operations of destructive malware (NotPetya) against a range of Ukrainian targets of computers in Ukraine's banks, electricity companies, newspapers, a nuclear facility, health ministry, the national railway and its postal service rendering the infected computers completely unusable. It took a long time to clean up and rebuild the relevant IT systems.

**Cyber Operations in U.S.** Russia has demonstrated its cyber-attack capabilities in the past in the infiltration of the US Democratic Party's National Committee mail server for theft of confidential emails, 2020 SolarWinds attack, ransomware hack of the Colonial pipeline etc.

### **Why Russia has not used its full cyber capabilities in Ukraine**

Experts' opinions are divided on why Russia has not used its cyber capabilities in Ukraine. Cyber means have not been effective at taking down the Ukrainian internet, telecommunications and mobile-phone systems offline. Russia's activities in cyberspace have been paltry or even nonexistent. Digital preparations for the invasion in Ukraine never occurred. Cyber operations were disorganised or lacked any real impact.

There are several theories. Some experts feel that Russia had been very slow to deploy cyber tactics in the war. The reasons could be:

- Putin did not feel the need to use cyber attacks in his strategy at this juncture in the war.
- He might want to avoid additional retaliation by the U.S. in the case of a cyberwar.
- Putin might be playing a long game and having his cyber operatives infiltrate various adversaries and gain footholds, waiting until he decides to launch a major cyber-attack.
- Russia would focus its resources on cyber reconnaissance missions than forceful attacks.
- Russians are keeping Ukrainian networks operating to assist their intelligence gathering.
- It is possible that cyber attacks are in progress and not understood in the

fog of a ground war.

- Russia believed that its army would conquer Ukraine in quick time and install a government that would need to have those services intact.
- When that doesn't happen, bombs were better options than cyber weapons to turn off the lights. In an all-out kinetic war, missiles offer a faster and more effective means of achieving strategic objectives than lines of code.
- Maybe Russia never had the capabilities that its adversaries attributed to it.
- Russia's lack of planning for the invasion may be the reason for these operational failures.
- Russian hackers are not agile enough to compromise the most important Ukrainian military, government and industry targets during fast-moving military operations.
- Russian Generals were skeptical of relying on cyber weapons.
- Maybe Ukraine's cyber defences successfully repelled the attacks, helped by their American allies.
- Due to the availability of high-quality, advanced personnel the Ukrainians are also good at cyberwarfare.
- Cyber weapons take years to develop, and these may be held in reserve for months or years. The weapons become useless if the vulnerabilities are patched in the meantime.
- In an all-out kinetic war, missiles offer a faster and more effective means of achieving strategic objectives than lines of code.

For militaries across the world integrating cyber with conventional operations in combat is a challenge. In Russia the military and intelligence cyber-ecosystem is teeming with units that compete with each other and lack co-ordinations. Incorporating cyber effects into kinetic operations is a difficult proposition for any military.

Greg Rattray, partner and co-founder of cyber advisory firm Next Peak, stated that one of the reasons there hasn't been a stronger cyber response from Russia is because "they aren't as deeply embedded and as capable as we had thought going into this, at least in the Ukraine." Perhaps Russian troops are dependent on Ukraine's own 3/4G networks for their own communication devices<sup>4</sup>.

However, some experts feel that this analysis is not correct. Russia has employed a coordinated cyber-campaign intended to provide its forces with an early advantage during its war in Ukraine. Cyberspace is an emerging domain of operations. Predetermined ideas of the role of cyber attacks on the battlefield have made it difficult for analysts to see the role cyber operations play within Russia's military campaign in Ukraine.

The claims that Russian cyber-operations were ineffective miss the bigger picture. In Ukraine, Russia has not yet shut down electricity or Internet connectivity. That does not mean Russia is not capable of such attacks, and Russia did not feel the need for such widespread, indiscriminate disruptions. Russian military units were probably reliant on Ukrainian civil infrastructure for their planned seizure of Kyiv and could not risk adverse effect to their own operations. Russia has considerably improved its ability to conduct comprehensive cyber operations in recent years and has actively invested in its cyber-capabilities.

Thomas Rid suggests that significant cyber-attacks have occurred, but they are more covert and insidious, and we're not focusing on them<sup>5</sup>.

So far, cyber operations against Ukraine have been far less than what everyone admits Russia is capable of. Some experts like Dmitri Alperovitch, the co-founder of the cybersecurity firm CrowdStrike, think that cyber warfare could still be on the horizon despite the lack of major attacks so far.

Alperovitch has high opinion of Russia's cyber operations capability. He said, "The reality is the Russian cyber forces carry quite a punch, they are highly capable, and whatever we may have done in Ukraine the last couple of months would not have stopped them. If we have some magical defensive capabilities, don't you think we would have used them here to defend our own networks against Russian forces? Are you going to tell me that in two months we were able to achieve in Ukraine what we weren't able to achieve in 30 years here?" That is just nonsense."

Professor Martin, who set up and led the UK's National Cyber Security Centre, wrote: "There seems to have been little effort, for example, to strike the core of Ukraine's internet infrastructure. Instead, the missiles rain, and the soldiers and tanks roll in. Similarly, the actions of pro-Ukrainian actors in defacing and taking down Russian websites may embarrass the Kremlin but hardly merit the much misused term of 'cyberwar'." He added, "Even though cyber operations

have featured to an unexpectedly small extent in the conflict so far, the West still remains at higher risk of serious disruption — as distinct from catastrophic attack — via the cyber domain than it was before the invasion."

## **Battle of Bits and Bytes**

Cyber warfare between Russia and Ukraine had started before the invasion began. It is still continuing. However, the intensity and its effect on both sides are not well known.

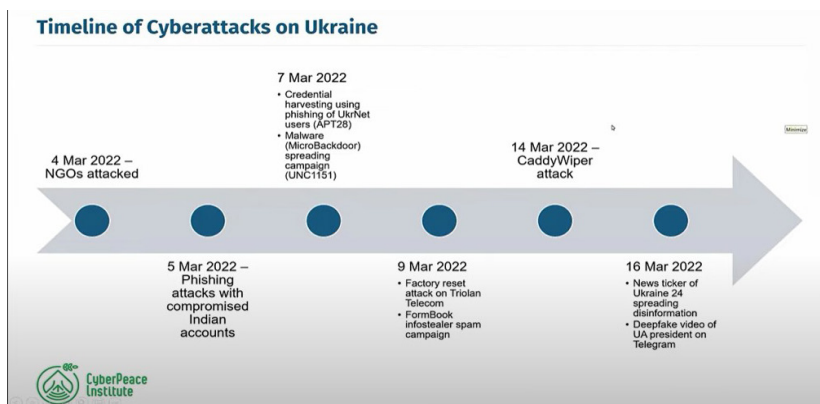
**Pre Invasion Cyber War.** In January 2022, wiper malware, a malicious software that erases the targeted computer's hard drive was detected in Ukrainian government networks and the private sector. New malware were distributed through phishing campaigns. There were a number of espionage attacks on high-value targets. Since February 15, 2022, Ukraine experienced more than three thousand DDoS attacks till February 24.

**Hacking of Satellite Communications.** During the early hours of February 24, 2022, a very significant attack on the KA-SAT satellite broadband network owned by an American satellite communications company took place. Somehow it is not getting then media attention. The KA-SAT network was hit by a mysterious cyber attack against the satellite's ground infrastructure that affected Ukraine and surrounding regions in Europe.

The satellite covers 55 countries providing fast internet connectivity, mostly in Europe. Among the affected Ka-Sat users were the Ukrainian armed forces, the Ukrainian police and Ukraine's intelligence service. ViaSat later stated that the incident started in Ukraine and then spread all over Europe, affecting 5,800 wind turbines in Germany and tens of thousands of modems across Europe.

Victor Zhora, the deputy chief of Ukraine's State Service of Special Communication and Information Protection, has characterised the satellite outage as "a really huge loss in communications in the very beginning of war."<sup>6</sup>

U.S officials told The Washington Post that the Russian military was responsible for cyber attack on the European satellite internet service that affected Ukrainian military communications. According to the Washington Post, the GRU, Russia's military intelligence agency, is considered to be behind the Viasat hack.



Source: <https://www.youtube.com/watch?v=ndno0Sq01Nc>

**IT Army of Ukraine.** Ukraine is not new to the cyber game. Shortly after Russia's invasion and annexation of Crimea in 2014, Ukrainian hackers came together under Ukrainian Cyber Alliance and started taking down Russian websites and leaking sensitive data. They hacked and leaked the email account of Putin's close advisor on the conflict in eastern Ukraine, Vladislav Surkov.

Ukraine was well aware of the threat posed by Russian hackers. Ukrainian President Volodymyr Zelensky Kyiv issued a decree to form offensive military cyber force on February 26, 2021. However, the organizations did not come up before the invasion.

Two days after Russia launched its invasion, Ukraine's vice prime minister and minister for digital transformation, Mykhailo Fedorov, called for "digital talents" since Ukraine was creating an IT army. He said, "We are creating an IT army. We need digital talents. All operational tasks will be given here: <https://t.co/Ie4ESfxoSn>. There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists."<sup>7</sup> He publicly called on volunteer hackers to take down another country's websites. He produced a list of 31 Russian government, bank, and corporation websites ready to go.

Many Ukrainian cyber professionals have volunteered to assist Ukraine's cyber operations. The volunteers are being organised through Telegram channels and other encrypted apps. Some 400,000 multinational hackers have volunteered to help counter Russia's digital attacks<sup>8</sup>.

The goals of this IT Army are:

- Defend Ukraine's critical infrastructure.
- Help the government with cyber espionage.
- Takedown Russian disinformation from the web.
- Targeting Russian infrastructure, banks and government websites.

Hackers targeted the Russian state-owned aerospace and defence conglomerate Rostec website, websites of several Russian banks, Russian power grid and railway systems, Russian businesses and other targets of strategic importance with widespread DDoS attacks. The bulk of Ukrainian cyber power seems to be coming from the IT Army<sup>9</sup>.

The volunteer hackers would not be able to match Russia's well-honed cyber capabilities, as they would not have the sophisticated offensive cyber tools and resources of state actors. But, capabilities of these groups should not be underestimated.

**Risk of Employing IT Army.** Some cybersecurity experts are justifiably worried about the employment of this volunteer army. Some of the reasons are:

- Lack of accountability regarding who is directing the battle plan and the overarching strategy.
- An army of 300,000 hackers will always include some bad hands. These volunteers might attack targets that are not of interest to the Ukrainian government. There can be spillover effects like ransomware. They could do something useless in the name of Ukraine, which could play directly into the Russians' hand.
- When hackers take orders from the Ukrainian army, they drop their status as civilians and could be considered combatants, making them legitimate military targets.

**Anonymous.** On the day of the invasion, February 24, 2022, the hacker collective Anonymous declared that it "was officially in cyber war" against Russia and has since claimed to have conducted covert attacks on the Russian Ministry of Defence, its Federal Security Service and Russian state television.



Anonymous  
@YourAnonOne

...

The Anonymous collective is officially in cyber war against the Russian government. [#Anonymous](#)  
[#Ukraine](#)

9:50 PM · Feb 24, 2022 · Twitter for iPhone

9,861 Retweets 1,429 Quote Tweets 48.5K Likes

Hacker group Anonymous has been linked to online attacks worldwide to punish governments for policies of which the hackers disapprove. Members are known as 'Anons' and are distinguished by their Guy Fawkes masks<sup>10</sup>.

On March 24, 2022, Anonymous announced that it hacked Russia's central bank and would soon release thousands of files. Earlier in March, members linked to the group offered Russian troops \$52,000 in Bitcoin if they abandoned their tanks on the battlefield.

It also claimed the theft and publication of Russian Department of Defence data, which may contain sensitive information helpful to fighters in Ukraine. Emails from Belarusian weapons manufacturer, Tetraedr and data from the Russian Nuclear Institute, have also reportedly been accessed. It is too early to determine how valuable these data may be.

Whether Anonymous will make a difference or not in this ongoing conflict is too early to assess. There are issues with the Anonymous group which may become problematic. They do not have any training in cyber warfare. There is a risk of significant unexpected collateral damage. What happens if one of the Anonymous attacks damages a critical infrastructure in Russia?"

U.K. authorities have cautioned amateur hackers not to join Ukraine's "IT Army" fearing that activists could be breaking the law or launch attacks that spiral out of control<sup>11</sup>.

**Russian Hackers.** Russia has effectively carried out offensive cyber operations, including cyber espionage, information and disinformation operations and

disruptive cyberattacks against Ukraine. It has not got the requisite media traction. Perpetrators include UNC2452, Turla, APT28, UNC530, UNC1151, UNC806, and other actors closely linked to intelligence services in Russia, Belarus and other countries.

Russian ransomware operators offered their services to the government, threatening to retaliate against governments that sought to punish Russia. These seem to be loosely controlled proxy groups and not a unified effort. A Ukrainian member of the Russian-linked Conti ransomware group, for instance, leaked the group's internal chat logs to counter the pro-Russian effort<sup>12</sup>.

At the beginning of the invasion in Ukraine, three strains of the Wiper malware simultaneously attacked local infrastructure. The virus deleted information and data from drives connected to the infection source. Some of the Wiper malware used were:

- HermeticWiper.
- WhisperGate.
- IsaacWiper.
- CaddyWiper.
- RURansom Wiper.
- Double Zero.

Some of the threat actors active in this cyber conflict are:

- UNC1151.
- APT28.
- Gamaredon.
- DanaBot.
- Conti RaaS Group.
- The Sandworm Team
- Strontium.

**Russia's Cyber Defence.** Though offensive cyber capabilities of Russia is well known, its defensive capabilities are not very clear. In the current conflict questions are being asked about Russia's cyber defence. Today it is Russia that is complaining of being the target of cyber offensives.

On March 2, 2022, Russia's cyber defence agency gave an alert that 17,500 IP addresses and 174 internet domains were involved in DDoS attacks on Russian sites and provided private organisations with mitigation measures. The website of the Russian foreign ministry, in a statement on March 29, 2022, said, "In fact, state institutions, the media, critical infrastructure facilities and life support systems are subjected to powerful blows everyday with the use of advanced information and communication technologies. At the instigation of the Kiev regime, an international call of anti-Russian computer specialists has been announced, in fact, forming offensive cyber forces. The bill for malicious attacks against us goes to hundreds of thousands per day."

## **Ukraine's Cyber War**

Ukraine started developing its national cyber strategy in 2021. Ukraine has taken back up of crucial data and services to protect the continuity of the economy and the presidency. Despite cyber attacks, Ukraine has been able to maintain communications with the outside world during the war can be taken as a victory for Ukraine.

Some of the successes claimed by hackers for Ukraine are given below.

- CyberPan Ukraine group working with the Ukrainian military and funded by sources in Israel and the U.S., claimed that it had found ways to disrupt Russian military units' navigation GLONASS system and is working to disrupt artillery fire. The group has several computer servers linked to Russian rockets.
- Russia's Era secure cell phones are not working because of poor communications technology and the destruction of many of the system's cell towers. This has forced many Russian units to use unencrypted phones, whose calls have been picked up by Ukrainian SIGINT agencies.
- Some hackers have published the personal information of 620 Russian intelligence officers and lists of military personnel accused of war crimes. Ukrainian news site Pravda was given a list of Russian soldiers and their personal information was published in full.
- It has been claimed that dozens of gigabytes of data have been leaked from the state-controlled energy companies Transneft and Rosatom, the Central Bank of Russia, government censor Roskomnadzor and state-owned media giant VGTRK. The leaks are part of a larger network of

amateurs helping Ukraine's war efforts with their keyboards.

Cyber security experts urge caution in drawing conclusions from hacked and leaked documents. False narratives can be planted as there is no guarantee the files are not tampered with<sup>13</sup>.

**Cyber Defence.** Ukraine has taken measures to augment its cyber security and improve the resilience of its cyber networks. Ukraine has been getting support from NATO, EU and global intelligence agencies. In 2018, it received ten million dollars to secure critical infrastructure from the U.S. State Department, with an additional eight million dollars in 2020 and a pledge for thirty million more and cyber assistance from the U.S. Army and NATO. Days before the invasion, Ukraine requested and received help from the European Union's Cyber Rapid Response Team to defend against cyber attacks by detecting when attacks occur<sup>14</sup>.

Ukraine has proved more resilient in cyberspace than what Russia anticipated. The head of U.S. European Command and NATO's supreme allied commander, Gen. Tod Wolters speaking during a Senate hearing told lawmakers that Ukraine's command and control of its military forces was intact. Wolters said that the U.S. and NATO had dramatically improved their offensive and defensive cyber tactics and ability to control the information environment throughout the Ukraine conflict.

**Role of Big IT Companies.** In an interesting development the behemoth IT companies have started working for Ukraine. Before the Russian invasion, Microsoft began working to help organisations in Ukraine to defend against an onslaught of cyberwarfare.<sup>15</sup>

Cisco and other U.S. companies are also working with Ukraine to kill large numbers of remote access Trojans that are utilised to gain remote control of computer systems. Google is now helping protect 150 websites in Ukraine from cyber attacks. A global cybersecurity company based in Romania, Bitdefender, has teamed up with its National Cyber Security Directorate to provide intelligence support to Ukraine.

Technology companies such as Twitter, Meta, TikTok and YouTube joined together to prevent the monetisation of disinformation by Russian-backed actors.

## **Role of U.S.**

U.S., especially its Cyber Command, has played a critical role in defending Ukraine's critical infrastructure and cyber networks before and during Russia's attack on Ukraine. It improved the resilience of Ukrainian networks by identifying cyber vulnerabilities and threats, shared intelligence, closely working with U.S. government and industry, and following extensive contingency planning<sup>16</sup>.

Gen. Paul Nakasone, Commander, U.S. Cyber Command and Director, National Security, in a written testimony provided to the Senate Armed Services Committee Agency on April 5, 2022, stated, "Coordinating with the Ukrainians in an effort to help them harden their networks, we deployed a hunt team who sat side-by-side with our partners to gain critical insights that have increased homeland defense for both the United States and Ukraine. When Moscow ordered the invasion in late February, we stepped up an already high operational tempo. We have been conducting additional hunt forward operations to identify network vulnerabilities. These operations have bolstered the resilience of Ukraine and our NATO Allies and partners. We provided remote analytic support to Ukraine and conducted network defense activities aligned to critical networks from outside Ukraine – directly in support of mission partners. In conjunction with interagency, private sector and Allied partners, we are collaborating to mitigate threats to domestic and overseas systems."<sup>17</sup>

On March 7, 2022, the New York Times reported that "forces from United States Cyber Command known as 'cyber mission teams' are in place to interfere with Russia's digital attacks and communications—but measuring their success rate is difficult."

## **U.S. Apprehension**

Russia is a cyber-superpower capable of disruptive and potentially destructive cyber-attacks with a serious arsenal of cyber weapons and hackers. Russia hosts the world's largest concentration of cyber criminals. In 2021, approximately three-fourths of ransomware's exponentially rising revenue went to cyber criminal groups in Russia. It exposed a soft underbelly of cyber vulnerability across the West<sup>18</sup>.

**Russian Capability.** The U.S. intelligence community, in 2019, in an unclassified assessment, said that Russia can disrupt electrical distribution centres in the United States for at least a few hours. Russian cyber operators gained access to several Fortune 500 companies and U.S. government agencies.

Some cyber security experts believe that the emphasis should be on ransomware attacks that can shut down a company's operations without attacking the systems that control the physical infrastructure. Inevitably, some attack will break through if an adversary like Russia puts enough resources behind it.

**Russian Actions against West.** Russia is suffering badly from American and European delivered anti-tank and anti-aircraft missiles on the Ukrainian battlefield. In the escalatory ladder, this action by the U.S. is not considered by the Russians a threat that could demand retaliatory kinetic action from them. The same cannot be said about combat aircraft or American troops entering Ukraine. This logic is not valid in the cyber world. There is a definite presence of U.S. CYBERCOM in Ukrainian cyberspace. The Russian may well be considering that the U.S. is in conflict with them crossing its virtual boundary.

Russia does not have to use cyberattacks that harm physical infrastructure in the U.S. It could cause chaos by hacking into the enterprise software of energy companies, as have been done in Colonial Pipeline attack. In mid-March, 2022, the FBI warned five U.S. energy companies that computers using Russian internet addresses had been scanning their networks in a possible prelude to more significant cyber attacks.

**Biden's Warning.** U.S. President Joe Biden has issued an urgent and ominous warning about Russian cyber attack. He has called on private companies and organisations in the U.S. to "lock their digital doors." He said, "Evolving intelligence suggests Russia might be planning cyberattacks against the U.S". The U.S. may have too many targets to defend them all, and some companies are not prepared.

**Attack on IT Companies.** Biden warned Putin that "we will respond", if Moscow attacks the U.S.'s critical infrastructure. However, critical infrastructure covers 16 sectors of the economy, including transportation, energy, dams, health care, the financial industry, water plants, government and others. Russian hackers, for more than a decade, have gone after targets in these fields.

Richard Clarke, who was an adviser on cybersecurity to President George W. Bush, told CNN, "Our declared policy is, if it's a big enough attack on us and it hurts us, we will use the conventional weapons response," Clarke argued that Russian attacks on US industries could be more destructive than attacks on the government organisations. He asked if the Amazon, Microsoft, Google cloud systems went offline what is the government going to do? Clarke himself gave the answer, "I can tell you if those clouds go down, the United States stops working, our economy stops working, the phones stop working -- we will find ourselves pretty soon in the dark ages if the internet goes down."

U.S. did not agree to the request of Ukraine to withdraw Google, Apple and the cybersecurity company Cloudflare from Russia. The U.S. knows that ordinary Russians might lose all access to independent news if they do not have access to Apple and Google app stores.

A State Department spokesperson stated, "It is critical to maintain the flow of information to the people of Russia to the fullest extent possible."<sup>19</sup>

## **NATO**

Some experts believe that Europe's critical infrastructure could be an attractive target for Russia as Europe is more dependent on Russian oil than the U.S. is. There has been apprehension that cyberattacks in Ukraine may spill over to neighbouring countries that are part of NATO. Could a cyberattack like this invoke Article 5 of its charter, the principle that an attack on one member of NATO is an attack on all members?

Jens Stoltenberg, NATO Secretary-General, is clear when he said at a news conference, "An attack on one will be regarded as an attack on all." However, he added that NATO would be cautious in assessing an attack and make sure a cyberattack on Ukraine that accidentally spilled over into Poland or Romania is not interpreted as an attack on those countries.

He also said it had been kept intentionally unclear what kind of cyberattack would rise to the level of invoking Article 5. NATO would not want to "give a potential adversary the privilege of defining exactly when we trigger Article 5."

## **U.S. Options**

According to the chairman of the analytical company Silverado Policy Accelerator, Dmitri Alperovitch, the U.S. will be left with no other option but to take an offensive cyber attack after the U. S. has exhausted all possibilities of economic sanctions against Russia. But that will put U.S. and Russia on a path that can quickly escalate into a hot cyberwar. The U.S. would like to avoid this scenario<sup>20</sup>.

The U.S. Intelligence agencies have penetrated the Russian higher military organisation to such an extent that they could correctly predict the day of the invasion and the Russian next move. Biden's warning about imminent Russian cyber attacker on U.S. critical infrastructure needs to be taken seriously.

Cyber security experts are divided in their opinion about the Russian cyberattack on the U.S. Some believe that the prospects of a large scale Russian cyberattack are low. Nearly 20 Specialists who spoke with CNN thought that while Russia is in a position to launch disastrous cyber attack, it is not likely to do so.

Others say, Russia's ability to conduct an impactful cyberattack in the US shouldn't be underestimated. The head of threat intelligence advisory at the cyber security firm IntSights, Paul Prudhomme, said, "We do need to consider this possibility as a low probability but high-impact scenario."

But it is a cat and mouse game. While it is true that Russians are prowling in the software of various structural areas of the U.S, the Americans are also lying in wait in theirs. The U.S. government for a long time, has warned that Russia has inserted malicious code in American networks, including the power grid, that could be triggered at a later date. But the U.S has done the same to Russia's Power Grid<sup>21</sup>.

While Russian cyberattacks tend to get maximum eyeballs, the most sophisticated attacks are carried out more professionally by countries like the U.S. and Israel. Stuxnet, in 2010, is a perfect example.

## **U.S. the Big Brother**

The U.S. is the biggest player in offensive cyber operations worldwide. It controls the world by its trillion dollars companies like Apple, Microsoft, Alphabet

(Google), Amazon, Meta (Facebook) and Twitter. The offensive cyber capabilities of NSA and USCYBERCOM are unmatched.

The case of hacking the hackers of China by the NSA is an example of the capabilities of NSA. The Chinese hacker group named *BYZANTINE CANDOR* focused mainly on breaking into the U.S. Department of Defense, while also spying on economic transactions of geopolitical interest, like oil deals. Tailored Access Operations (TAO) cell of NSA was tasked<sup>22</sup>.

The TAO found and hacked those same computers from which they hacked American targets. TAO gained insight into the PLA's activities against the U.S. government, defence contractors, foreign governments, etc.

For the first time in the history of cyber conflict, the U.S might find cyber operations a better option for strategic action in a foreign country. The operations might involve disabling servers of Russian cyber warfare units (those within the GRU) or the interruption of criminal ransomware groups. They might cut off the computer networks that support Russian commercial or financial operations that circumvent sanctions<sup>23</sup>.

The Russians may well be aware of the American's might in the cyber world and would be hesitant to get involved in a major cyberwar with the U.S. However, this is in a speculation stage. With time things might get clearer.

## **Conclusion**

There is a tendency to hype up cyber threats. Despite the perceived success of Russia's 2016 election interference campaign and the SolarWinds attack, evidence of the impact of cyber operations is missing. Russian cyber operations lean towards low-cost disruption efforts that rely on cyber patriots and criminal hackers than their ability to carry out sophisticated degradation campaigns.

It is a challenging and prolonged process to build an extremely sophisticated cyber option like Stuxnet. It does not come cheap in spite of the proliferation of cyber weapons globally. Cyber is an excellent tool for sub conventional conflict, where you are trying to hit back at the other party without escalating to a kinetic conflict. Tactical objectives are not only about disrupting services, but also about intimidation, distraction and confusion. Once conflict begins, cyber becomes

much less useful. Physical attacks are more disruptive than cyber attacks.

The last word on cyber warfare in the ongoing war in Ukraine has not been said.

## Endnotes

1. Julia Voo et al, National Cyber Power Index 2020, Belfer Center for Science and International Affairs Harvard Kennedy School, September 2020 available at: [https://www.belfercenter.org/sites/default/files/2020-09/NCPI\\_2020.pdf](https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf)
2. Cyber Capabilities and National Power: A Net Assessment, IISS, June 28, 2021 available at: <https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power>
3. <https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/>
4. Sam Sabin And Laurens Cerulus, Why Ukraine's phones and internet still work, Politico, March 7, 2022 available at: <https://www.politico.eu/article/why-ukraines-phones-and-internet-still-work/>
5. Thomas Rid, Why You Haven't Heard About the Secret Cyberwar in Ukraine, New York Times, March 18, 2022
6. Corin Faife, Russian military reportedly hacked into European satellites at start of Ukraine war, The Verge, Mar 25, 2022, <https://www.theverge.com/2022/3/25/22996187/russian-military-hack-viasat-internet-satellite-ukraine>
7. Mykhailo Fedorov (@FedorovMykhailo) February 26, 2022, [https://twitter.com/FedorovMykhailo/status/1497642156076511233?ref\\_src=twsrc%5Etfw](https://twitter.com/FedorovMykhailo/status/1497642156076511233?ref_src=twsrc%5Etfw)
8. Ukraine war, The Strategist, Australian Strategic Policy Institute, March 14, 2022.
9. For the first time in history anyone can join a war: Volunteers join Russia-Ukraine cyber fight", CNBC, March 14, 2022.
10. Harry Howard, , | Hacking collective Anonymous declares 'cyber war' against, February 25, 2022 available at: <https://www.dailymail.co.uk/news/article-10549849/Hacking-collective-Anonymous-declares-cyber-war-against-Vladimir-Putins-government.html>
11. Dan Milmo, Amateur hackers warned against joining Ukraine's 'IT army', The Guardian, March 18, 2022 available at: <https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army>
12. Brandon Valeriano et al. Putin's Invasion of Ukraine Didn't Rely on Cyberwarfare. Here's Why, Cato Institute, March 7, 2022 available at: <https://www.cato.org/commentary/putins-invasion-ukraine-didnt-rely-cyberwarfare-heres-why>
13. Patrick Tucker , Ukrainian Hackers Take Aim at Russian Artillery, Navigation Signals, Defense One, MARCH 30, 2022 available at: <https://www.defenseone.com/technology/2022/03/ukrainian-hackers-take-aim-russian-artillery-naviga->

tion-signals/363854/

14. Colin Demarest, US Cyber Command reinforces Ukraine and allies amid Russian onslaught, Apr 8, available at: <https://www.c4isrnet.com/cyber/2022/04/07/us-cyber-command-reinforces-ukraine-and-allies-amid-russian-onslaught>
15. Tom Burt, Disrupting cyberattacks targeting Ukraine, Microsoft, April 7, 2022 available at: <https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia/>
16. Marcus Willett, Russia–Ukraine:Pressing the rightbutton at the righttimem, IISS available at: <https://www.iiss.org/blogs/analysis/2022/03/russia-ukraine-pressing-the-right-button-at-the-right-time>
17. Posture statement of Gen. Paul M. Nakasone, commander, U.S. Cyber Command before the 117th Congress, U.S. Cyber Command, April 05, 2022 available at: <https://www.cybercom.mil/Media/News/Article/2989087/posture-statement-of-gen-paul-m-nakasone-commander-us-cyber-command-before-the/>
18. Jack Detsch and Mary Yang, Russia Prepares Destructive Cyberattacks, Foreign Policy, March 30, 2022 available at: <https://foreignpolicy.com/2022/03/30/russia-cyber-attacks-us-ukraine-biden/>
19. Joseph Marks, Cyber conflict in Ukraine is growing more complex by the day, The Washington Post, March 16, 2022 available at: <https://www.washingtonpost.com/politics/2022/03/16/cyber-conflict-ukraine-is-growing-more-complex-by-day/>
20. Dmitri Alperovitch on the risks of escalation, The Economist available at: <https://www.economist.com/by-invitation/2022/02/23/dmitri-alperovitch-on-the-risks-of-escalation>
21. David E. Sanger and Nicole Perlroth, U.S. Escalates Online Attacks on Russia's Power Grid, The New York Times, June 15, 2019 available at: <https://www.ny-times.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>
22. Michael Riley and Dune Lawrence, Hackers Linked to China's Army Seen From EU to D.C., Bloomberg, July 26, 2012 available at: <https://www.bloomberg.com/news/articles/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor>
23. Lucas Kello, Monica Kaminska , Cyberspace and War in Ukraine: Prepare for Worse, Lawfare, April 14, 2022 available at: <https://www.lawfareblog.com/cyberspace-and-war-ukraine-prepare-worse>

## 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](mailto:info@vifindia.org),

Website: <https://www.vifindia.org>

Follow us on [twitter@vifindia](https://twitter.com/vifindia)