WORLD RISK & GOVERNANCE

INSIGHTS

Russo-Ukrainian War On The Cyberspace

Omkar Moharir, *Junior Risk Analyst*

14 Mar 2022

I. INTRODUCTION

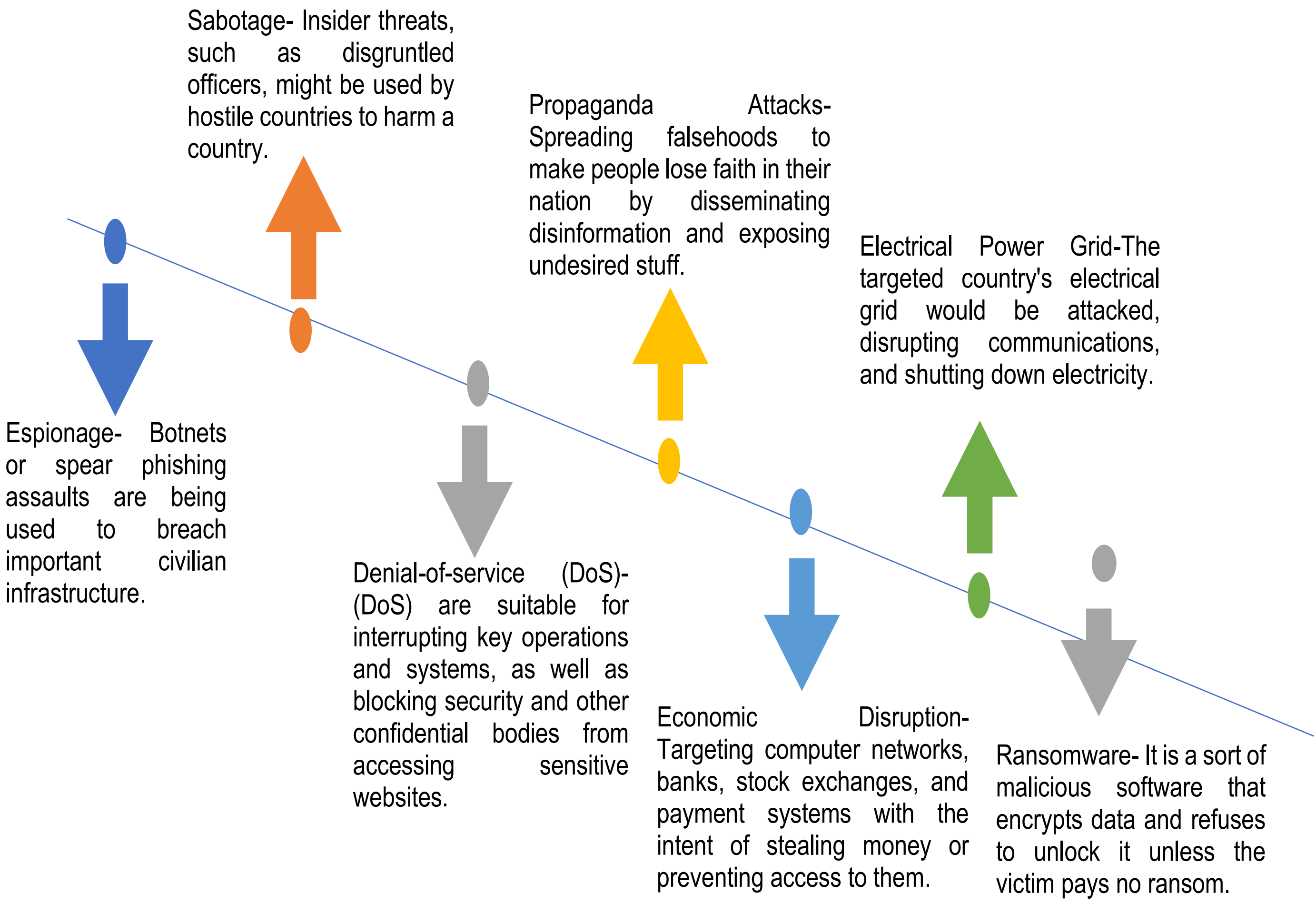
Russia began a complete invasion of Ukraine on 24 Feb. After a long-running Russian military build-up (from Sep 2021), as well as several Russian requests for security measures and legislative limitations against Ukraine joining NATO, had preceded the campaign. Since then both sides are involved in a tough battle to regain the control of Ukraine, which has led to the one of the biggest humanitarian and refugee crisis in Europe after World War II.

Till now Ukraine has shown strong resistance against Russian aggression and Russians are yet to take Kyiv despite possessing extraordinary military power as compared to Ukraine. Ukraine has successfully managed to gain support from many countries and has managed to corner Russia in multilateral organizations like United Nations (UN). Volunteers across the globe are assembling to fight for Ukraine against Russian invasion.

One of the important features of the Russo-Ukraine conflict has descended fifth-generation war. So called Future Wars which have components of cyber capabilities including the utilisation of social media platforms in the creation certain narrative against each other.

The Russo-Ukraine conflict appears to have all the components for a cyberwar. Moscow and Kyiv are competing for the highest geopolitical stakes, and both governments have extensive information technology and computer hacking capabilities. The world is witnessing one-of-a-kind war that includes huge data manipulation and disinformation spreading across borders. This report is specially focused on how cyberwarfare has changed the landscape of conventional warfare and how future wars will be fought using cyber capabilities and utilising the social media platforms. Even though that doesn`t change the nature of warfare, using arms and military capabilities, but cyberwarfare has the capabilities to affect critical infrastructures and speeding propagandas. How the world in interconnected due to cyberspace and how by targeting the cyberspace business continuity can be affected.

II. CYBER WAR METHODS



Espionage- Botnets or spear phishing assaults are being used to breach important civilian infrastructure.

Sabotage- Insider threats, such as disgruntled officers, might be used by hostile countries to harm a country.

Denial-of-service (DoS)- (DoS) are suitable for interrupting key operations and systems, as well as blocking security and other confidential bodies from accessing sensitive websites.

Propaganda Attacks- Spreading falsehoods to make people lose faith in their nation by disseminating disinformation and exposing undesired stuff.

Economic Disruption- Targeting computer networks, banks, stock exchanges, and payment systems with the intent of stealing money or preventing access to them.

Electrical Power Grid-The targeted country's electrical grid would be attacked, disrupting communications, and shutting down electricity.

Ransomware- It is a sort of malicious software that encrypts data and refuses to unlock it unless the victim pays no ransom.

III. CYBER ATTACKS BY RUSSIA AND ALLIES

From sanctions compliance to supply chain disruption to business interruption, Russia's assault on Ukraine poses a wide variety of dangers. The cyber risk has sparked widespread concern, and the risk scenario is constantly evolving, even though the specifics of increased cyberattack activity are not yet completely understood and may be primarily unfolding beneath the surface as the actual invasion continues. The invasion of Ukraine by Russia is being fought not just with bombs, but also with bytes, as cyber warfare plays an increasingly important role.

For decades, Russia has been one of the world's most capable cyber powers. Russian state-sponsored hackers have been suspected of being behind some of the most sophisticated cyberattacks publicly reported since the Moonlight Maze attacks against the US Department of Defense in the 1990s. They are, in particular, To achieve their geopolitical objectives, they are known to attack opposing key infrastructure.

The Conti ransomware operators are the most well-known cybercriminal outfit to overtly support Russia. They have a history of actively targeting US healthcare organisations. They've been known to hack Managed Service Providers (MSPs), perform big game hunting (targeting major businesses), and launch multi-stage attacks (combining many attacks). As part of the attack, malware types were used, as well as double and triple extortion (data theft mixed with ransomware attack).

Russia has used its cyber capabilities to spread disinformation, propaganda, espionage, and harmful cyberattacks around the world. To carry out these Russia has many units that are involved in operations. Various security and intelligence agencies oversee it. Organizations affiliated with the Russian government, cybercriminal groups headquartered in Russia and surrounding states, and organisations affiliated with the Belarussian government are all possible danger groups currently linked to the Russia-Ukraine war.

In early Feb, Russia started a series of distributed denial of service (DDoS) operations against Ukrainian websites. The attacks, which were apparently carried out by the Russian military intelligence organisation GRU, targeted Ukrainian banking and defence websites. The strikes occurred as tensions between Ukraine and Russia grew.

Russia has continued to perform DDoS attacks on Ukrainian defence ministry websites on a regular basis, and in the first week of March, Russian groups were discovered utilising DanaBot, a malware-as-a-service platform, to launch DDoS attacks. It's unknown who these organisations are or if they're linked to the Russian government.

The Microsoft Threat Intelligence Center (MSTIC) has discovered evidence of a devastating malware campaign in Ukraine that has targeted many companies. On 13 Jan 2022, this virus was first detected on target systems in Ukraine.

PRO-RUSSIA

HermeticWiper — This is a new type of disk-wiping malware (at least one version has the filename Trojan attached to it). Killdisk) that was used to strike Ukrainian groups just before a Russian invasion on 24 Feb 2022

WhisperGate- is a novel type of disk-wiping malware with three stages/parts: a bootloader that corrupts detected local discs, a Discord-based downloader, and a file wiper. The WhisperGate bootloader is a companion to the WhisperGate file-wiper. Both permanently destroy the victim's data and try to pass themselves off as ransomware. Whispergate has been spotted hitting Ukrainian organisations just before the Russian invasion on 24 Feb.

-On Feb 24, 2022, Russia unleashed a wiper, codenamed IsaacWiper, on Ukrainian government networks, coinciding with the Russian invasion of Ukraine. The attacks came soon after the HermeticWiper attacks, and they appeared to be more targeted than the HermeticWiper attacks. Long before the wiper was deployed, the impacted firms had been penetrated.

BELARUSIAN GROUP UNC1151 & ITS METHODS

On 14 Jan, Ukraine's government suspects Belarusian threat actor UNC1151 of launching a cyberattack against over 70 government websites. In advance of Russian troops crossing the border into Ukraine, hackers

Ukraine`s Computer Emergency Response (CERT-UA) Team has confirmed that **MicroBackdoor** malware was used in a cyber-attack campaign targeting Ukrainian government entities . CERT-UA reported that government organisations have been the target of many malicious attacks in a statement made on 07 Mar.

APT28, a Russian threat actor, has launched a credential phishing campaign aimed against users of UKRNet, a famous Ukrainian media company. The effort appears to have been halted after being discovered by Google's Threat Analysis Group (TAG).

At least 30 university websites in Ukraine were also hacked in a targeted attack apparently carried out by threat actors known as the **'Monday Group**,' which has reportedly publicly backed Russia's recent activities. The group, whose members refer to themselves as 'the Mx0nday', have targeted the WordPress-hosted sites more than 100,000 times since the invasion.

defaced the websites, putting menacing comments such as "be afraid and expect the worst." The attack is thought to have been a deception to divert attention away from more dangerous attacks. UNC1151 was also discovered in early March starting a phishing attempt targeting the Ukrainian and Polish governments and forces, though it is unknown whether they were successful in gaining access to any networks.

IV. CYBER ATTACKS BY UKRAINE AND ALLIES

Ukraine's government is seeking volunteers from the hacker community to assist in the protection of critical infrastructure and offensive operations against Russian state-sponsored hackers. “Ukrainian cybercommunity! It’s time to get involved in the cyber defense of our country,” reads the post published on the forum. “We have an army inside our country,” “We need to know what they are doing.” Yegor Aushev, the co-founder of a cybersecurity company in Kiev, told Reuters news agency that he wrote the post at the request of a senior Defense Ministry official who contacted him.

Following Russia's invasion of Ukraine, a Twitter message by "**Anonymous**" called on hackers all around the world to attack Russia. Anonymous, a secretive online group, appears to be entering the Ukraine-Russia crisis by declaring cyber war on Russian President Vladimir Putin and the Russian government. In the days that followed, the account claimed credit for deactivating the websites of Russian energy giant Gazprom, state-controlled Russian news network RT, and a slew of Russian and Belarusian government organisations, including the Kremlin's official website.

Following tweets claimed responsibility for interrupting Russian internet service providers, releasing data and emails from Belarusian weapons manufacturer Tetraedr, and shutting down a gas supply provided by Russian telecoms company Tvingo Telecom. "Anonymous has ongoing operations to keep the Russian government website offline, and to push information to the Russian people so they can be free of Putin's state censorship machine," the account user said in a Twitter.

Volunteer organisations organised through social media and Telegram channels have aided Ukrainian efforts in cyberspace. One of the most significant efforts by the Ukrainian government to coordinate cyberespionage activity is the IT Army of Ukraine. Individuals or organisations use the details provided by the IT Army to undertake attacks against the designated targets, which are posted to a Telegram channel with hundreds of thousands of subscribers. The IT Army has conducted widespread DDoS operations against additional strategic targets, including the websites of many Russian banks, the Russian power infrastructure, and the Russian railway system. The IT Army looks to be the source of the majority of Ukrainian cyberpower

PRO-UKRAINIAN GROUPS CYBERATTACKS

The Belarusian Cyber Partisans, who initiated cyberattacks on Belarusian train systems in Jan in protest of Russian force deployments in the nation, appear to have continued their campaign against Belarusian railways. The assaults took down websites that were used to purchase tickets and may have encrypted data on switching and routing systems, while the scope and seriousness of the attacks beyond website takedowns were unknown.

The **RURansom Wiper**, which first appeared on 01 Mar 2022, is one of the first wipers used by the pro-Ukrainian hacktivists, and it could herald a new phase in the continuing cyber battle against Russia. Despite its name, RURansom is a wiper that does not allow victims to pay to have their systems decrypted. The malware appears to look for a Russian IP address on the victim's PC, and if it doesn't locate one, it appears to terminate operation. The malware creators also appear to be actively releasing new versions of the wiper, and it may only grow more potent over time.

V. WAR OF DISINFORMATION

Most social media feeds have been flooded with posts regarding the Russia-Ukraine conflict. While some of these posts come from legitimate news organisations, many of them are part of disinformation campaigns spreading inaccurate information that is passed off as reality to deceive.

PRO-UKRAINIAN DISINFORMATION CAMPAIGN

The **"Ghost of Kyiv**," for example, may have shot down several Russian MIGs. However, the narrative has yet to be verified, and the viral image is a pilot modelling a prototype helmet. Furthermore, despite Russian rumours to the contrary, Ukrainian President Volodomyr Zelensky has not fled the country. Disinformation and misinformation have the potential to play a large part in this war, given the level of contemporary technology and the geopolitical atmosphere.

Even though misinformation is common in wars, the amount of disinformation in this fight is far greater than usual. Furthermore, it appears that much of the disinformation is coming from third individuals who are not affiliated with either militaries or governments. Individuals across the world are utilising social media to spread a great deal of false information. Some of the misinformation is spread on purpose to benefit Russia or Ukraine. Ukraine entered the fight as the typical underdog, which drew widespread support. However, it is a slippery slope for Ukraine to go from underdog to lost cause, and many will no longer consider it worthwhile to support. As a result, tweets about how skillfully the Ukrainian military and people are fighting the Russians have flooded social media. Meanwhile, the Russians were regarded as a powerful military force when they entered the war. Despite the war's failures, many Russian supporters are circulating footage of Russian military victories to keep the country's image of being invincible.

Supporters on both sides, for example, are releasing fake videos of the Russian and Ukrainian Air Forces achieving victory.

PRO-RUSSIAN DISINFORMATION CAMPAIGN

In a viral video, a Ukrainian fighter jet shoots down a Russian MiG fighter jet over a Ukrainian city. Meanwhile, another viral video showed a Russian MiG fighter evading a barrage of SAMs. Both videos were, in fact, from the popular videogame Arma 3 and were afterward taken down from social media. Individuals, on the other hand, are often unintentionally spreading false information. The "series of wars" produces a lot of ambiguity about what's going on the ground. Furthermore, Ukrainian soldiers are unlikely to be carrying cell phones to prevent having their locations triangulated, as the Russians did in 2014. Even if they have cell phones, Russian militaries' commanders have prohibited their troops from using social media. As a result, there is little news from the front lines. People are turning to online sources for imagery for memes and posts in the absence of actual pictures from the fighting. They find historical photos, misunderstand them as being from the current conflict, and use them in their posts to support their claims.

VI. BUSINESS CONTINUITY DUE TO CYBER WARFARE

Conflict in Ukraine, whether military, cyber, or hybrid, will have long-reaching consequences for businesses far beyond the region's boundaries. As a business leader, you've probably already considered whether there are individuals at risk, operations that could be harmed, or supply networks that could be disrupted. The conflict in Ukraine poses the most serious cyber threat that the United States and Western firms have ever faced. A Russian invasion would result in the broadest and most severe sanctions ever imposed on Russia, which regards such measures as economic warfare. Russia will not sit idly by but will strike back asymmetrically with its extensive cyber capabilities. Following previous US Cybersecurity, and Infrastructure Security Agency (CISA) warnings about the risks posed by Russian cyberattacks for US critical infrastructure, the CISA recently issued a warning about the risk of Russian cyberattacks spilling over onto US networks. In the event of sanctions and market disruptions, the European Central Bank (ECB) has warned European financial institutions of the potential of retaliatory Russian cyber-attacks.

- Several big multinational company`s security and intelligence teams have stated that they are anticipating Russian cyberattacks and evaluating the possibility for second and third-order consequences on their operations.
- Some businesses have stated that they expect an uptick in attacks and frauds because of the Ukraine crisis, with risk evaluations often based on whether the business has direct connections to Ukrainian national banks or other important infrastructure.

- According to Ukraine's Ministry of Foreign Affairs, more than 100 of the Fortune 500 corporations rely on Ukrainian IT services at least in part, with numerous Ukrainian IT firms ranking among the top 100 global outsourcing alternatives for IT services.
- Malicious actors have been known to take advantage of such events by publishing phishing links on social media with ostensibly legitimate news updates or email scams ostensibly soliciting charitable donations.

VII. ASSESSMENT

For a long time, analysts, insurance companies, and other organisations have been mapping the key – perceived – dangers and hazards to enterprises each year. Cyber catastrophes have steadily become much more major concerns for enterprises as digital technologies have become more crucial, ranging from data breaches and cyberattacks to unexpected outages of critical systems. Given the United States' and European Union's joint backing for Ukraine, the reach of a cyberwar might be enormous. Due to the spill-over effect, large-scale cyber skirmishes can become worldwide. There is some precedence for how a spill over may appear. In 2017, Ukraine's airports, trains, and banks were impacted by a suspected Russian assault including the malware "NotPetya." NotPetya, on the other hand, did not remain in Ukraine. It quickly spread over the world, infecting — and for a time effectively shutting down — a wide range of multinational corporations, including the global shipping business Maersk, the pharmaceutical giant Merck, FedEx's European affiliate TNT Express, and others. When it comes to infrastructure resilience. A major cyberattack can have the same effect as a natural catastrophe, taking off critical infrastructure and causing a chain reaction of disasters. It may, for example, be similar to the Texas winter freeze of 2021, which caused widespread disruptions, power outages, and over 200 fatalities. It could have been a lot worse. "Texas' electrical infrastructure was 'seconds and minutes' away from a catastrophic breakdown that could have left Texans in the dark for months," according to the Texas Tribune.

Companies should seek assurances that our infrastructure can recover quickly following a cyberattack prior to the assault, and have those assurances validated by independent auditors. Cyber terrorists are motivated by politics and want to cause widespread disruption. They aim for every technology-controlled key infrastructure that might cause severe service disruptions to generate fear and economic downfall for the state and businesses.

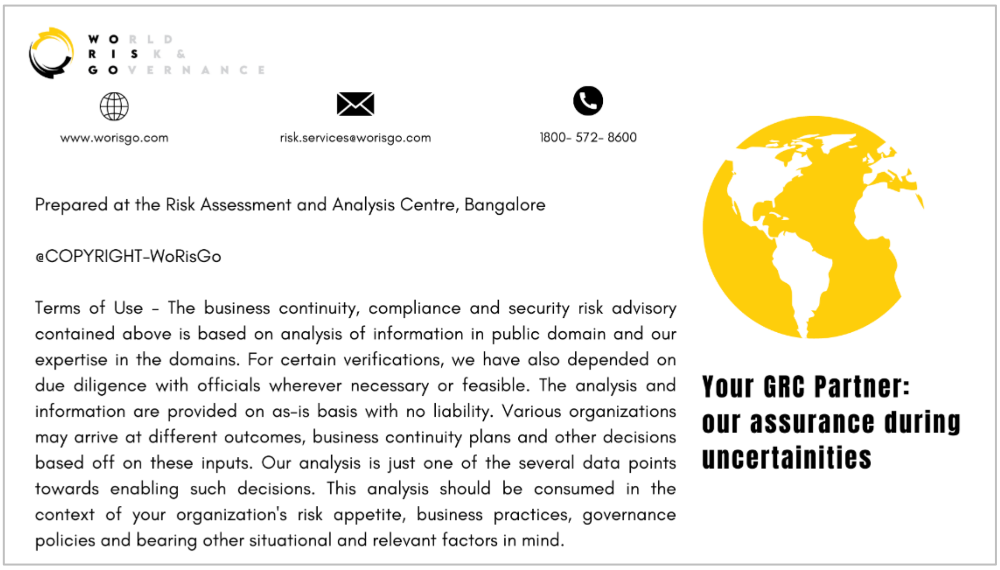
The present crisis has strained relations between the United States and Russia, raising the prospect of a larger European confrontation. Due to alliance security obligations, tensions are anticipated to rise between Russia and nearby NATO member nations, with the United States likely to be involved. Furthermore, the crisis in Ukraine will have far-reaching consequences for future collaboration on vital problems like as arms control, cybersecurity, nuclear non-proliferation, energy security, counterterrorism, and political solutions in Syria, Libya, and elsewhere. The invasion of Ukraine by Russia has had a substantial impact on American and European businesses with service activities in the region, according to industry experts, the services of almost 1,00,000 highly qualified IT and technology employees in Ukraine, Belarus, and Russia have been disrupted due to the persons who were previously worked in GBS (Global Business Service) centres and with third-party service providers. In the region, there are considerable worries regarding business continuity and data security. As ongoing tensions in Eastern Europe have an influence on IT service providers in these regions, their investments and benefits may transfer to global IT centres like India.

VIII. CONCLUSION

The world is drive by technological advancement because of Cyber Space, the world is interconnected as it was never. Businesses across the globe are hugely relying on cyber capabilities to continue their work process. Cyber space has become so crucial factor to the technological driven world, which has created several threats and loopholes for business continuity. Data is the new asset for the world. Every Country, Company, or individual wants to protect their data. To protect the huge amount of Data, nations and businesses should work together to deter their adversaries. The more we rely on cyber capabilities more countermeasures are required to contain cyber warfare. The current Russo-Ukraine conflict is the perfect example how futuristic battles will take place, which will have both cyber and physical components.

ABOUT THE AUTHOR

Omkar Amol Moharir is Junior Risk Analyst at WoRisGo and is responsible for Americas focusing on risk and threat assessments. He has completed his Post-Graduation in Geopolitics and International Relations, Manipal Academy of Higher Education, Karnataka, and completed Bachelors in Journalism and Mass communication from IP University, New Delhi, He Believes that his knowledge about the field has been gained through extensive research analysis in the areas of geopolitics, diplomacy, foreign policy, National Security, Counter terrorism, Risk Analysis, Marketing, Advertising and Public Relations



WORLD
RISK &
GOVERNANCE

🌐 www.worisgo.com

✉ risk.services@worisgo.com

☎ 1800- 572- 8600

Prepared at the Risk Assessment and Analysis Centre, Bangalore

@COPYRIGHT-WoRisGo

Terms of Use - The business continuity, compliance and security risk advisory contained above is based on analysis of information in public domain and our expertise in the domains. For certain verifications, we have also depended on due diligence with officials wherever necessary or feasible. The analysis and information are provided on as-is basis with no liability. Various organizations may arrive at different outcomes, business continuity plans and other decisions based off on these inputs. Our analysis is just one of the several data points towards enabling such decisions. This analysis should be consumed in the context of your organization's risk appetite, business practices, governance policies and bearing other situational and relevant factors in mind.

Your GRC Partner:
our assurance during
uncertainities