9500 GROUP

Cyber Operations in the Ukraine War

Cyber – Influence Operations

In the Russia-Ukraine War

12-Apr-2022

Table of Contents

Introduction

Cyber-based hostile influence campaigns are aimed at influencing target audiences by promoting information and/or disinformation over the internet, sometimes combined with cyber-attacks which enhance their effect. Such hostile influence campaigns and operations can be considered an epistemological branch of Information Operations (IO) or Information Warfare (IW).

Hostile influence campaigns, much like Cyber-attacks, have also become a tool for rival nations to damage reputation or achieve various military, political or ideological goals. Much like in the cyber security arena, PR professionals and government agencies are responding to negative publicity and disinformation shared over the news and social media. In times of war, the frequency and intensity of such activities grow ten folds, thus providing a rare opportunity for researchers to analyze the effectiveness of different types of operations.

We use the term **cyber based** hostile influence campaigns, as we include in this definition also cyber-attacks aimed at influencing (such as hack and leak during election time), while we exclude of this term other types of more traditional kinds of influence such as diplomatic, economic, military etc.

This on-going ever-updated paper will focus only on the cyber-influence operations (hence Cyfluence, as opposed to cyber-attacks that aim to steal information, extort money, etc.).

Because of disinformation and the “fog of war” it is too early to analyze and assess the real situation, so this current paper focuses on the first month of the war, and is more of a list of events than an analysis.

Executive Summary

Before Russia invaded Ukraine on February 24, observers expected cyber-attacks to play a large role in the conflict. However, despite Russia's strong cyber capabilities, and despite a variety of large scale attacks against Ukrainian government websites, banks, critical infrastructure and military targets, there has been relatively (to the expectations) little visible impact.

If Russian cyber-attacks were really less effective (yet to be proven) then there might be several reasons why Russia hasn't launched full force attacks at the beginning of the war, among them the higher efficacy of kinetic attacks and difficulties in planning and executing massive cyberattacks on a short timeline.

At the beginning of the war, there was a prominent usage of DDoS attacks against governmental websites, aiming to seed fear and disarray. Meanwhile, phishing campaigns and wipers attacks were used to target internal networks and computers of government and military officials. At that early stage of the war, more aggressive network take-downs or attacks probably did not fit with Russian objectives and Russia could even be leaving the broadband network active for its own means for intelligence gathering and influence operations. In late March, however, major internet takedowns occurred in Ukraine, possibly marking a change in strategy of Russian cyber efforts.

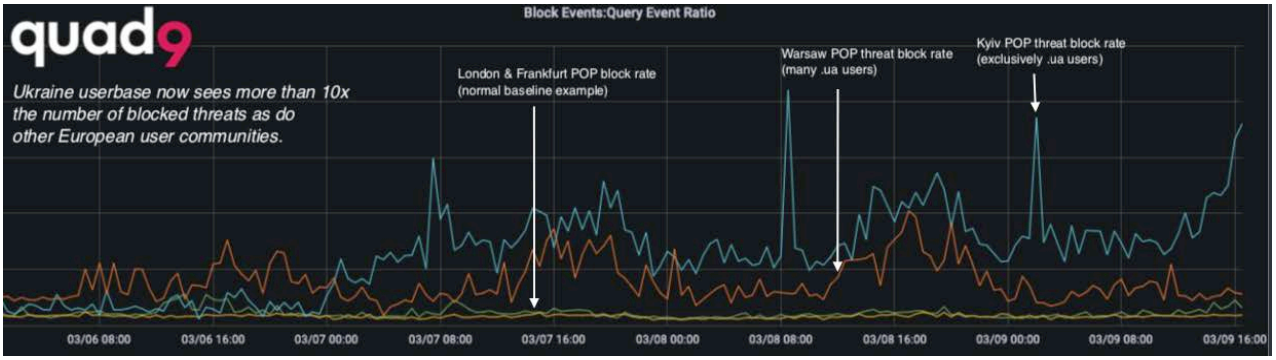
Apart from "official" Russian hacking groups, cyber gangs from different countries and without official relations to the Russian government stood by the side of Moscow. In addition, groups from Arab countries and Latin America took responsibility for several cyber-attacks in the first month of the war. The same happened on the other side, while Ukraine official and unofficial hackers attacked Russian targets, while calling hackers from all over the globe to join them.

On the other side of the war, Ukraine has pursued a unique strategy in cyberspace, attempting to mobilize international sentiment and create an army of cybersecurity professionals and hacker to defend the Ukrainian infrastructure and attack military targets and critical infrastructure in Russia.

Below are two timelines aiming to depict the volume of Russian cyber operations in the beginning of the war:

- Major cyber-attacks by Russia against Ukraine between January 14th to February 27th 2022[1].

- Blockage of DNS requests for known-bad domains used by malicious software, phishing websites and more between March 6th to 9th 2022. The blue line represents Ukraine, the orange line represents Poland, the others represent the UK and Germany as baselines. [2]



[1] https://www.slideteam.net/ukraine-and-russia-cyber-warfare-it-russian-cyber-operations-against-ukraine-timeline.html
[2] https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/

Fogs of war, mainly created by the Ukrainian government, inhibit proper analysis of the cyber field. Therefore, we present the pieces of news as they are, without digging into their full meaning. However, one might say that from what is already known so far, the Russian cyber-attacks aimed at influencing Ukrainian leaders and the Ukraine population have at best limited effect. Even if Russia has succeeded in achieving tactical victories, overall, it has failed strategically.

A more complete understanding of the cyber aspect of the Russian invasion of Ukraine is probably not possible until after the conflict ends; however in this document we aim for drawing a preliminary overview of the role of cyber-attacks for influence (Cyfluence) in the conflict.

Russian Cyber Attacks

Types of Attacks

Russia's Cyber-attacks role in the Conflict

According to Info Security, cyber-attacks have already played a significant role in the conflict, both before and since the Russian invasion of Ukraine. In the build-up to the invasion, security companies observed many attacks that were "aligned with Russia's strategic objectives." These involved "undermining the Ukrainian government, intimidating and demoralizing the Ukrainian population, causing confusion and disrupting the everyday lives of Ukrainian citizens."

The principal methods utilized by Russian state-sponsored and nexus threat groups were DDoS attacks, destructive malware attacks, website defacements and fraudulent messaging. Additionally, a significant uptick was noted in dark web adverts related to Ukraine; for example, the sale of data related to the Ukrainian Ministry of Foreign Affairs. These attacks, which primarily targeted government and critical sectors, such as banking, were highly coordinated, for instance: a simultaneous DDoS and wiper malware attack the day before the invasion began.

An Update on the variety of Russian Cyber-attacks

Google's Threat Analysis Group (TAG) warns of government-backed attack, alerting Ukrainian users that they have been the target of government backed hacking, largely emanating from Russia. The Russian activity ranges from espionage to phishing campaigns, including a GRU's several large credential phishing campaigns targeting ukr.net users[3]. The phishing emails were sent from a large number of compromised accounts (non-Gmail/Google), and included links to attacker controlled domains. In two recent campaigns, the attackers used newly created Blogspot domains as the initial landing page, which then redirected targets to credential phishing pages.

In addition, TAG continues to see **DDoS** attempts against numerous Ukraine sites, including the Ministry of Foreign Affairs, Ministry of Internal Affairs, as well as services like Liveuamap that are designed to help people find information.

[3] UkrNet is a Ukrainian media company.

Russia "Pre-positioned" Cyber-Attacks for the Invasion

Info Security reported that the UK and US governments quickly attributed DDoS attacks on Ukrainian organizations in mid-February 2022 to Russian intelligence. A National Cyber Security Centre (NCSC) missive said it is "almost certain" that the attacks which took place on February 15 and 16 were the work of the Russian Main Intelligence Directorate (GRU). "The US government believes that Russian cyber-actors likely have targeted the Ukrainian government, including military and critical infrastructure networks, to collect intelligence and pre-position to conduct disruptive cyber activities."

Vulnerability Exploit Attempts Surge against Ukrainian Websites

The websites of at least 30 Ukrainian universities have been compromised by a threat actor expressing support for Russia, according to Info Security. Total attempts to exploit WordPress vulnerabilities in Ukraine jumped to 144,000 on the day of the Russian invasion, roughly three times the number of daily attacks from earlier in the month. The culprit was named as a Brazil-based threat group known as

Ukraine Attacked with Wiper Malware

Info Security reports that Ukraine is being targeted by new data-wiping malware. Hundreds of machines across at least five organizations in Ukraine were found infected with **HermeticWiper**. The attack took place just hours after several of the country's government and banking websites were knocked offline in a series of DDoS attacks.

According to ESET, further analysis of HermeticWiper has revealed a worm constituent that propagates the malware across the compromised network and a ransomware module that acts as a distraction from the wiper attacks. As an anti-forensic measure, HermeticWiper is also designed to hinder analysis by erasing itself from the disk by overwriting its own file with random bytes.

Second New 'IsaacWiper' Data Wiper Targets Ukraine

A new data wiper malware has been observed deployed against an unnamed Ukrainian government network; a day after destructive cyber-attacks struck multiple entities in the country preceding the start of Russia's military invasion. ESET dubbed the new malware "**IsaacWiper**," which it said was detected on February 24 in an organization that was not affected by **HermeticWiper** (aka FoxBlade).

Ukrainian Targets Hit by another Destructive Malware Variant

Info Security reports of yet another destructive malware variant targeting Ukrainian machines, the fourth so far. The "**CaddyWiper**" malware was seen on a few dozen systems in a "limited number of organizations". It erases user data and partition information from attached drives, and does not share any code similarities with the previous variants discovered. Interestingly, CaddyWiper avoids destroying data on domain controllers. This is probably a way for the attackers to keep their access inside the organization while still disturbing operations.

Threat Actors

The Conti ransomware group

According to Info Security, since the invasion started, a number of cyber-criminal groups have supported Moscow. For example, the Conti ransomware group announced that they would support all actions of the Russian government during the invasion of Ukraine, would put in all efforts to resist cyber-attacks against Russia and would target the critical infrastructure of Russia's enemies in retaliation for attacks against Russia.

APT28

According to Google's Threat Analysis Group (TAG) FancyBear / APT28, a threat actor attributed to Russia GRU, has conducted several large credential phishing campaigns targeting a Ukrainian media company users.

theMx0nday

A Brazil-based threat group that has expressed online support for Russia. It has a history of stealing sensitive information from its victims and used infrastructure from a privacy-centric hosting provider run by Pirate Bay co-founder.

Attacks on Government and military targets

Attack on Ukrainian Government Websites Linked to GRU Hackers

On 23 February, the day before Russian forces invaded Ukraine, most key Ukrainian government institutions had their **websites attacked in a DDoS campaign**. The websites of the Ukrainian parliament, Ministry of Foreign Affairs, and Council of Ministers, and the Security Service of Ukraine, were all unreachable. One website that was not affected by this specific attack was the website of the Office of the President of Ukraine.

Independent threat in cooperation with Bellingcat has identified a web service, serving as a C&C center, which has played a role in past cyber-attacks linked to Russia. The same website also hosted cloned copies of a number of Ukrainian government websites, including the main webpage of the Office of the President. Notably the cloned version of the site of the Ukrainian president was modified to contain a clickable "Support the President" campaign that, once clicked, downloads a package of malware to the user's computer. It is not certain what the purpose of the malware payload is at this time, nor whether the payload was operational or simply a placeholder for different malware to be deployed at a crucial moment.

In addition, according to CFR, a destructive wiper attack impacting hundreds of machines was reported in Ukraine and two neighboring countries. The USA, the UK and Ukraine attributed those attacks to Russia.

Vermin Hacking Collective Hits Ukrainian Government and Military

On March 17, 2022, the government emergency response team of Ukraine CERT-UA revealed that the Ukrainian **government infrastructure** was hit by a massive spear-phishing campaign aimed at SPECTR malware delivery. The campaign was launched by Vermin (UAC-0020) hacking collective associated with the so-called Luhansk People's Republic (LPR). Vermin hackers are believed to be acting on behalf of the Moscow government and being an operational unit of the Russian cyber warfare against Ukraine.

According to SOC Prime, the Vermin collective disseminated malicious emails with the subject "supply" among the state bodies of Ukraine. As a result of the cyber-attack, the compromised computer is exposed to harmful modular software dubbed SPECTR, which applies a set of malicious components SPECTR.Usb, SPECTR.Shell, SPECTR.Fs, SPECTR.Info, and SPECTR.Archiver to spread the infection further.

Cyber Attacks Hit Ukrainian Government Agencies

According to CFR, Ukraine was hit by a series of attacks **against government agencies**, which top Ukrainian cybersecurity officials have said were **the largest cyberattacks ever to hit the country**. The officials also said that the attacks bore the hallmarks of an operation by a foreign intelligence service, although they declined to single out Russia. The DDoS attacks were primarily targeted at government websites and **managed to take down most services**, for at least two hours.

Ukrainian IT Army Hijacked by Info-stealing Malware

Security researchers are urging pro-Ukrainian actors to be wary of downloading DDoS tools to attack Russia, as they may be booby-trapped with info-stealing malware, Info Security claims. The researchers detected posts on Telegram offering DDoS tools which were actually loaded with malware. One such tool, dubbed "Liberator", is offered by a group calling itself "disBalancer". The file offered on the Telegram page ended up being an infostealer. The malware in this case dumps a variety of credentials and a large amount of cryptocurrency-related information, including wallets and metamask information, which is commonly associated with NFTs.

Attacks on Media

Russian Hackers Compromise Ukrainian News Sites

According to Info Security, multiple Ukrainian news websites were hacked by Russian hackers, leaving the 'Z' symbol on display, with the hackers apparently compromising Ad services.

Attacks the Banking Sector

Cyber Attacks Hit Ukrainian Banks and Government Agencies

According to CFR, Ukraine was hit by a series of attacks **against banks**. The DDoS attacks were primarily targeted at banks and **managed to take down most services**, including ATMs and websites, for at least two hours. U.S. intelligence officials have warned that Russia has likely infiltrated far deeper into Ukrainian systems. Some cybersecurity officials suggested that the relatively obvious DDoS attacks could be a distraction while Russian hackers lay the foundations for much more serious attacks.

Attacks on Communication

Ukraine Suffers Significant Internet Disruption Following Cyber-Attack

Ukraine's national telecommunications provider has been hit by a significant cyber-attack, leading to the "most severe" disruption to internet connectivity in the region since the start of the conflict with Russia, according to Info Security. The telecommunications provider explained it temporarily restricted access to private users and businesses to ensure internet services to critical infrastructure and armed forces were not interrupted. The available network activity appeared to show a gradual decline in connectivity, rather than a cliff-edge drop typical of DDoS or a ransomware attack at the core of the network. This would suggest a supply chain attack where endpoint devices such as home routers are slowly being taken out.

Attack on Ukraine Telecoms Provider

Russian hackers used compromised employee credentials to launch a cyber-attack that severely disrupted internet services in Ukraine, Info Security claimed. Ukrtelecom senior said that Russia accessed the account of an employee in a region "recently temporarily" occupied. Once they gained access, the hackers tried to disable Ukrtelecom's equipment and servers to gain control over its network and equipment. There was also an attempt to change the passwords of employees' accounts and of logins to access equipment and firewalls.

Viasat: Denial of Service Attack Impacted Tens of Thousands

A denial-of-service (DoS) attack on a leading satellite communication provider on the day of Russia's invasion hit tens of thousands of customers in Ukraine and elsewhere, Info Security reports. Viasat said the "multifaceted and deliberate" cyber-attack took the majority of its thousands of Ukrainian customers offline. It began when some hijacked modems and other customer equipment inside Ukraine began firing high volumes of targeted malicious traffic, making it difficult for legitimate modems to remain online.

Subsequent investigation and forensic analysis identified a ground-based network intrusion by an attacker exploiting a misconfiguration in a VPN appliance to gain remote access to the trusted management segment of the KA-SAT network. The attacker moved laterally through this trusted management network to a specific network segment used to manage and operate the network, and then used this

network access to execute legitimate, targeted management commands on a large number of residential modems simultaneously. Specifically, these destructive commands overwrote key data in flash memory on the modems, rendering the modems unable to access the network, but not permanently unusable.

General Reports

Tracking Cyber Operations and Actors

CFR offers an accounting of observed actors operating in the conflict, along with major cyber operations taken by each side. Several examples:

- DDoS Attacks against Ukrainian banking and defense websites.
- Wiper attacks (WhisperGate malware) on the systems of the Foreign Ministry and the Ukrainian cabinet.
- Phishing attacks of UKRNet users for credentials stilling.

Belarusian Cyber Attacks

A Belarus-Linked Cyfluence Campaign Targeting Ukrainians

According to Politico, Meta researchers found that a hacking group known as Ghostwriter (AKA UNC1151) gained access to Facebook and Instagram accounts of prominent Polish and Ukrainian government and military organizations, including politicians, military leaders and journalists. Using these accounts, Ghostwriter posted disinformation designed to make the Ukrainian military appear weak. These posts included a fraudulent YouTube video showing Ukrainian soldiers surrendering.

According to CFR, UNC1151 had defaced over 70 Ukrainian government websites and installed a backdoor onto government system. This enabled the attackers to attempted hacking the email accounts of Ukraine military personnel in a mass phishing attack. Once the hackers infiltrated military personnel's accounts, they leveraged the compromised address books to send more malicious emails.

Ghostwriter Group Targeted NATO Refugee Effort

Info Security reports that a new phishing campaign linked to a disinformation threat group, is targeting European governments as they try to manage an influx of Ukrainian refugees. First spotted on February 24, the original phishing email was sent using a compromised account belonging to a member of the Ukrainian military. The email itself piggybacked on news of a recent UN Security Council meeting, and contained a malicious XLS macro later determined to deliver the SunSeed malware. The file itself was spoofed to appear as if it contained a recently discovered 'kill list' of Ukrainian figures drawn up by Moscow.

The observed email messages were limited to European governmental entities. The targeted individuals possessed a range of expertise and professional responsibilities. However, there was a clear preference for targeting individuals with responsibilities related to transportation, financial and budget allocation, administration, and population movement within Europe. This campaign may represent an attempt to gain intelligence regarding the logistics surrounding the movement of funds, supplies, and people within NATO member countries. It could be that the group is gathering evidence to help craft more narratives about migrants and refugees intended to sow discord across Europe, a tactic it has used before.

Ukrainian Cyber Attacks

Actors

Ukraine Asks for Hackers' Help

The government of Ukraine has asked for volunteers from the country's hacker underground to help protect critical infrastructure and conduct cyber spying missions against Russian troops, Reuters reports. The volunteers are divided into defensive and offensive cyber units. The defensive unit is employed to defend infrastructure such as power plants and water systems. The offensive volunteer unit is helping Ukraine's military to conduct digital espionage operations against the Russian forces.

Anonymous Hacking Group Declares "Cyber War" Against Russia

Info Security reports that the hacktivist group Anonymous has declared "cyber war" against Vladimir Putin's government following the Russian invasion of Ukraine. Shortly after, the group claimed responsibility for taking down Russian government websites, including the Kremlin and State Duma. According to CFR, the group claimed to have disabled sites run by Russian state-owned media and appears to have targeted pro-Russia media outlets several times. Anonymous also claimed to have hacked several major Russian broadcasters and streaming services. On March 10, Anonymous announced it had breached the systems of Roskomnadzor, the Russian agency responsible for monitoring and censoring media.

The IT Army of Ukraine Cyber Operations

According to CFR, A crowdsourced community of hackers endorsed by Kyiv officials - the IT Army of Ukraine - attacked Russian banks, the Russian power grid and railway system. According to Info Security the group also attacked the website for the Moscow Stock Exchange, and has launched widespread DDoS attacks against other targets, such as the Russian state-owned aerospace and defense conglomerate Rostec. The bulk of Ukrainian cyberpower appears to be stemming from this group.

The IT Army has functioned by posting important targets to a Telegram channel with hundreds of thousands of members, while individuals or groups use the details provided to launch attacks against the specified targets.

Attacks on Infrastructure

Moscow Exchange Downed by Cyber-Attack

The website of the Moscow Stock Exchange was offline and inaccessible, Info Security reports. The Ukraine IT Army has claimed responsibility. On the hit list of the newly formed "army" are the websites of 31 Russian businesses and state organizations, including those of Gazprom, Lukoil, three banks and several government websites.

Attacks on Media Outlets

Anonymous Hacking Group attacks on Russian Media Outlets

According to CFR, Anonymous claimed to have disabled sites run by Russian state-owned media and appears to have targeted pro-Russia media outlets several times over the past two weeks. Anonymous also claimed to have hacked several major Russian broadcasters, including state-run television channels Russia 24, Channel 1, Moscow 24, and streaming services Wink and Ivi. Programming on these services was interrupted by clips from the war in Ukraine.

On March 10, Anonymous announced it had breached the systems of Roskomnadzor, the Russian agency responsible for monitoring and censoring media. The group leaked over 360,000 files, including guidance on how to refer to the invasion of Ukraine.

Info Security reported that Anonymous had targeted the website of the Russian-state controlled international television network RT.

Russian TV Stations Hacked

According to Info Security, hackers have taken over Russian TV channels and media sites to broadcast messages opposing Russia's invasion of Ukraine. State-owned news agency TASS and daily newspaper Kommersant were temporarily knocked offline in late-February 2022, while St Petersburg-based news outlet Fontanka's content was replaced with a message addressed to Russia's citizens calling them to stop the war.

Anonymous, which declared "cyber war" against Russia, claimed responsibility for the hacks on TASS, Izvestia, Fontaka, RBC and Kommersant. All the sites suffered outages, while several displayed messages. Anonymous claimed to have also hack into the network of Russian company Tvingo Telecom, disrupting its supply of gas.

Cyber Security / Defense

EU Deploys Cyber Response Unit to Ukraine

Info Security reports that the EU is deploying a newly formed Cyber Rapid-Response Team (CRRT) to Ukraine to help the country combat Russian threat actors as troops start pouring over the border. Lithuania will be leading the coalition of six EU countries – which also includes Croatia, Poland, Estonia, Romania and the Netherlands – in order "to help Ukrainian institutions to cope with growing cyber-threats."

Ukraine's Electric Grid Still an Easy Target for Russian Hackers

Politico reports that the U.S. and its allies poured tens of millions of dollars during the past seven years into helping Ukraine shore up its electric grid against a Russian cyberattack, while Ukrainian authorities launched a massive program to harden their cyber defenses. The Ukrainian government has also made an effort to work with the private companies that it will need to help coordinate response to an attack on the grid, as not all energy companies are state-owned.

Glossary

Information Operations - the employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making." Information Operations (IO) are actions taken to affect adversary information and information systems. IO can sometimes be considered as a part of Soft Warfare.

Hybrid Warfare - a known strategy which blends conventional warfare (kinetic), irregular warfare and cyber-warfare with other Soft Warfare parts like influencing methods, fake news dissemination, diplomacy, lawfare and foreign electoral intervention, to mention a few.

Cyber Warfare – commonly known as the use of digital attacks to cause harm and/or disrupt vital computer and information systems. There is a debate among experts regarding the definition of cyber warfare, and even if such a thing exists.

Cyfluence Attack – a cyberattack that aims to amplify or enhance an influence effort, as opposed to cyber-attack that aim to steal information, extort money, damage military capability etc.

Soft Warfare – all warfare disciplines that are not kinetic (i.e. no physical attack of sort of shooting, using explosives, poisoning etc.), such as cyber warfare, economic warfare, diplomatic warfare, legal warfare (lawfare), psychological warfare and more.

Misinformation - false, inaccurate, or misleading information that is communicated regardless with intention to deceive. Examples of misinformation are false rumors or straight-out lies or dissemination of known conspiracy theories – on purpose.

Disinformation - false or misleading information that is spread and distributed deliberately to deceive. This is a subset of misinformation. The words "misinformation" and "disinformation" have often been associated with the concept of "fake news", which some scholars define as "fabricated information that mimics news media content in form but not in organizational process or intent".

Hostile Influence Campaign (HIC) - An information operation sought to influence targeted audience for a hostile cause.

Disclaimer and Limitation of Liability

Copyright and License of Product

This report (the "Product") is the property of Intercept 9500 Ltd. ("Intercept") and is protected by Israel and international copyright law and conventions. User acknowledges that access to the Product is limited to the License terms set forth herein and any expansion must be in writing. The granting of the License to access and use the Product is conditioned on User's agreement not to disclose, copy, disseminate, redistribute, or publish the Product, or any portion of or excerpts thereof to any other party.

User shall have the right to use the Product solely for its own internal information purposes. Reproduction of the Product in any form or by any means is forbidden without Intercept's written permission.

User agrees to maintain all copyright, trademark and other notices contained in the Product. User agrees that it shall not use Intercept's name or any excerpts from the Product in the promotion of its products or services.

Disclaimer of Warranties

Intercept does not make any warranties, express or implied, including, without limitation, those of merchantability and fitness for a particular purpose, with respect to the Product. Although Intercept takes reasonable steps to screen the Product for infection by viruses, worms, Trojan horses or other code manifesting contaminating or destructive properties before making the Product available, Intercept cannot guarantee that the Product will be free of infection. Intercept does not make any warranties, express or implied, of whatsoever nature with respect to the Product or to the accuracy of any conclusions set out in the Product.

Accuracy of Information

The information contained in the Product has been obtained from sources believed to be reliable and are provided by Intercept on an "as is" basis. To the full extent permissible by applicable law, Intercept disclaims all warranties, express or implied, of whatsoever nature including, but not limited to any warranties as to the accuracy, completeness, quality or adequacy of any such information, any conclusions set out in the Product and any translations in the Product. The reader assumes sole responsibility for the selection of the Product to achieve its intended results. The opinions expressed in the Product are subject to change at any time without notice.

Limitation of Liability

To the extent permitted under applicable law, in no event will Intercept be liable in any way for:

1. damages of any kind, including without limitation, direct, incidental punitive, special or consequential damages (including, but not limited to, damages for lost profits, business interruption and loss of programs or information) arising out of the use of or inability to use the Product, or any information provided in the Product, regardless of whether or not Intercept has been advised of the possibility of such damages;
2. Any claim attributable to errors, omissions or other inaccuracies in the Product or interpretations thereof;
3. actions taken or not taken by any person or entity as a result of the review by such person or entity of the Product or information contained therein or as a result of the interpretation of the Product or information contained therein by such person or entity.

Indemnification

User agrees to indemnify, defend and hold harmless Intercept, its affiliates, licensors, and their respective officers, directors, employees and agents from and against all losses, expenses, damages and costs, including reasonable .attorneys' fees, arising out of the use of the Product by User or User's account.

Third Party Rights

The provisions regarding Disclaimer of Warranty, Limitation of Liability and Indemnification are for the benefit of Intercept, and its licensors, employees and agents. Each shall have the right to assert and enforce those provisions against a User.

General Provisions

Any provision in any memorandum received by Intercept in connection with the Product which is inconsistent with, or adds to, the provisions of this Agreement is void. Neither the parties' course of conduct or trade practice will modify the terms of this Agreement. If any provision of this Agreement is determined by a court of competent jurisdiction to be invalid, all other terms and conditions shall remain in full force and effect.

Governing Law

This Agreement and the resolution of any dispute arising hereunder shall all be governed and construed in accordance with the laws of the state of Israel, without regard to its conflicts of law principles. User consents to the jurisdiction of the courts of Tel-Aviv.