SWCP Portal

March 2022

The Fog of Cyberwar

Over the last decade, the ***SWCP PORTAL*** has carried many articles on **cyberwar**. We traced its development from the first attacks on physical infrastructure, the **Stuxnet virus** used against Iran's atomic centrifuges in 2010, to the attacks on **US pipelines** just last year.

Along the way, we've covered related aspects of online conflict, such as **hacking**, **phishing**, **fake news** and targeting of **social media** and how they could be fought. But never before have we seen all these things unleashed within a real, live conventional war.

With Russia's invasion of Ukraine, we are witnessing **information war** in real time, and will doubtless see many more ploys and feints in the hard days to come. So this issue looks at the basics of warfare in cyberspace, what it means, and how to try to keep ourselves safe in these difficult and dangerous times.

The first victim

"***Truth is the first casualty of war***." This is an **adage** which appeared in print during the First World War, attributed to many people because it's so obviously correct. The present conflict dramatically confirms this; for the truth was under deadly attack long before any rockets flew with Russian President **Putin's lies** about not wanting war and his increasingly **bizarre claims** to justify his invasion.

President Biden adopted a daring strategy to publish what our intelligence services actually knew to counter these claims, often before the Russians published them. Rumors of **Ukrainian attacks** on the separatist regions, or the **mass graves** supposedly found there, for instance, were debunked and defused even before any claims were made in the Russian press. Meanwhile, commercial satellite pictures **showed** the steady build-up and movement of army units encircling Ukraine.

All of this must have raised a lot of eyebrows in the Kremlin; however, it does not seem to have deterred Putin at all. Yet, even if they endangered US "**sources and methods**" of intelligence gathering, the revelations kept the Russians from completely controlling the narrative and thus prepared the planet.

By proactively leaking Russian plans, the US climbed above the "**fog of war**" – a much-used phrase graphically describing the situational uncertainties that bedevil combatants. For confusion made by that fog has always been a part of battle. In the age of gunpowder, it was quite literal, as the first volley of cannonfire could obscure a battlefield with enough smoke that commanders could only guess what was really happening out there.

Many cyberwar activities are meant to penetrate the modern fog to discover the foe's real plans, abilities, and situation or to thicken it to better hide one's own. For cyberwar is merely an extension of humanity's age-old tendency for violence into cyberspace.

Old tricks, new tech

The purpose of the bag of dirty tricks people have always kept handy for desperate fights remain the same: **espionage**, to spy out the enemy's concealed plans and abilities; **sabotage**, to secretly disrupt their means to achieve those ends; and **propaganda**, to openly spin tales about events and intentions, exaggerating one's own righteous victories and cause against the foe's wicked failures.

Only the means have changed. Espionage and sabotage are now done by phishing and hacking, while propaganda campaigns compete across social media. This creates a cyberfog which is far broader and more confusing than the kind known by generals on horseback, for the entire planet is now involved.

What is most unique about today's situation is that the struggle is playing out online, and the internet is already a major field of battle for the hearts and minds of the world.

The war is still in its early stages and the crisis may easily escalate both unpredictably and dangerously, but here is the situation at the time of this writing. Remember, **both sides** may resort to any of these methods to some degree, and to countermeasures, also.

It was **widely thought** that the conflict would begin with an onslaught using the net to knock out power and communications. After all, Russia took down Ukraine's power grid twice already, in **2015** and **2016**, and in **2017** infected it with **powerful malware** as well.

Surprisingly, this still hasn't happened yet. Russia's main assaults on Ukraine's communications systems have been repeated missile attacks on **Kiev's TV tower**. The power, net, and phone systems all still work, which has given a great boost to the defenders' ability to get their story and pleas out to the world.

The world has responded, too, with near-universal condemnation of the invasion, while Russia fights to control the story within its borders by **cracking down** on protesters.

Most likely, the Kremlin hoped for such a swift, easy victory that they did not want to break what they would soon need during the occupation. Or perhaps, since both sides have had years to **prepare** for cyberwar, the Russians were **deterred** by US threats of reprisal if Western infrastructure was attacked.

Maybe measures to harden the net over the last several years have succeeded. Whatever the reason, the situation may change, as Ukraine has called for a **volunteer IT army** of hackers, a global crowdsourced effort claiming that **400,000 volunteers** are working while **Russian volunteer hackers** fight back.

Their latest **announced targets** are the Russian GPS system and the railway of Putin's close ally, Belarus. Meanwhile, the **Anonymous** hacker group has **hacked Russian TV** and websites; the teen who tracked Elon Musk's plane is now following the **planes and yachts** of the oligarchs on Twitter; and the Ukrainians have **released data** on some 120,000 Russian soldiers with **videos** on TikTok that is even leading to identifying some of the invaders through facial recognition.

Big Tech strikes back

Like every other major Western corporation, Big Tech firms scrambled to cut ties with Russia and to block their access to markets and media. But some have done even more.

At the request of the vice prime minister, Elon Musk made his **satellite internet** service available to Ukraine and sent them a truckload of Starlink receivers, though they can be **jammed** or **targeted** for attacks.

Just before the actual invasion, Microsoft spotted a new piece of **malware**, designed to wipe data, aimed at Ukraine's government. Blocking the code within 3 hours, they then shared the info with front line states. It seems that recent efforts to bring companies and governments to work together on **cybersecurity issues** were not a waste of time.

Facebook tried to block Russian trolls and their disinformation mills like RT, and **stop hackers** from taking over Ukrainian military and important officials' accounts. Meanwhile, Twitter's **automatic censorship** controls were tricked by complaining Russian botnets causing the shutdown of **open source intelligence** accounts tracking army movements that provided important fact-checking data.

Even before the attacks, the federal government issued warnings of hostile hacking from **banks** to **satellite communications** and **GPS systems**. They **urged** law enforcement, the military, and other parties to prepare by patching all systems and reporting **unusual online activity** to authorities.

In this war, we are all targets. Be vigilant against **phishing attempts** to break into systems big and small. Keep supplies on hand like for any disaster, back up your files, and check with SWCP Tech Support if concerned.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994

505-232-7992** | **swcp.com** | Tech support: **help@swcp.com
5021 Indian School NE, Ste. 600, Albuquerque, NM 87110

*Please click on **bold blue type** in text for links to sources.*