SWCP Portal

October 2022

Avoiding Cyber Doom

Just as it is hard to comprehend the size and girth of the globe from our comfy chairs, so too is the difficulty of trying to grasp the scale of the conflicts seething through the world online from our friendly little screens.

Without question, however, the largest and most significant struggle on all levels now is the war between **Russia and Ukraine**. These states are fighting each other not just on land, sea, and air, but in cyberspace, with weapons of espionage, sabotage, and propaganda refitted for the new digital battlefield.

The fight is taking place in a weirdly wired world, one where **webcams** often catch evidence of gruesome atrocities that expose official lies while unwilling Russians can **call Ukraine** to find out how to surrender and rented satellites **monitor** battlefield claims.

Yet even as the threat of **nuclear annihilation** looms like a black cloud over Ukraine, so does a potential "**cyber doom**", an apocalypse that comes to pass over the internet.

Fears of an internet armageddon

The threat of attacks on vital entities like government or industrial websites has been around a long time. Spying was the first concern. Only when it became clear that online attacks could **overwhelm** enemy servers with a rapid bombardment of requests was the concept of war across the internet first raised.

Those potentials greatly increased in 2010 with the **Stuxnet virus**. The first real cyber weapon, Stuxnet caused Iran's uranium centrifuges to physically destroy themselves, thus slowing their nuclear program by years. However, as the malicious code sabotaged internet-connected industrial controllers, it could be adapted by state-backed hackers to crash a whole juicy range of essential utilities.

As the authorities do not like to publicly share data, little is known about most attacks. Not all such events are even admitted. But the three cyber attacks that the US **most feared**, including the pipeline shutdown that spiked our gas prices, all had Russian involvement.

Years before the war started, a **cyber Cold War** had emerged that has so far been a stalemate, for the US responded to intrusions into our basic utilities by infiltrating our foes'.

Mutual assured destruction thus again may deter a potential – albeit now cyber – apocalypse. Another reason may be that since digital weapons can be used only once before countermeasures are devised, all sides are saving the very worst hacks for the last resort.

So methods that worked before were tried again. The Russians hit most of Ukraine's state online systems and also caused power outages for years after seizing Crimea. The worst such attack was the **NotPetya** wiper virus in 2017 that caused ***$10 billion*** in damage to companies doing business with Ukraine. But during the invasion, Russia deployed other wipers that destroyed data just to sow chaos.

That operation also hit computers in NATO members Latvia and Lithuania, thus posing a possible risk of escalation. Crippling cyber attacks on a member state can and may warrant an **armed response** from the alliance, but the threshold is dangerously indefinite.

At the start of the war, President Biden was presented with **options** for massive cyber attacks against Russia. Meant to disrupt the invasion, they included such exploits as disabling the net or the electric grid in Russia, or even messing with their railway switches.

The "intelligence" officials proposing this bold plan of action claimed that since the attacks would disrupt networks but not destroy anything, they would fall short of being acts of war. Not that the United States would ever admit responsibility anyway. Fortunately, the President seems to have wisely decided not to play around with cyber brinkmanship.

Reusing the old **Cold War hotline** between the US and Russia to prevent cyberwar was agreed on back in 2013. Without a safe way to talk, the chaos in communications caused by an accident or miscalculation could result in panic and disastrous overreaction.

So what of "**cyber doom**" then? It is interesting that the term originated a decade ago, but has been mainly used since then by **cybersecurity firms** to debunk the idea of an overwhelming internet assault while scaring people with the threat of it to gain support.

Though the US has moved to a more aggressive posture, think tanks are now calling for "**cyber restraint**", noting that historically, online offensives have not changed enemies' behavior much and often invited retaliation. Perhaps the Russians have a similar doctrine.

While hopeful to think so, it is far too early to relax, however. The situation could change at any moment unpredictably and with lightning speed, especially if Putin feels his back against the wall. And there are other factors in play, too, beyond anyone's control.

Taking up digital arms

During the invasion, the Russians may have hesitated to destroy infrastructure they might need later. However, many **Western analysts** were surprised that initial cyber attacks by Russian hackers were not worse.

It was widely expected that along with the blitz, there would be a massive online onslaught, which did not happen. Not only that but the Russian military has relied on **insecure communications** since the start which Ukraine has either listened in on or jammed.

The fight online isn't completely one-sided, either. Many **Kremlin websites** were taken down in denial-of-service attacks, too.

Ukraine quickly set up **secure communications** of their own with US commands while SpaceX foiled Russian attacks on **StarLink**. By keeping their national network functioning and connected, the outside world has been able to watch as it all happens, so that Ukraine has won widespread sympathy. In this, the Russians have unwittingly helped the most by committing one senseless, brutal **war crime** after another, spattered around the planet daily across the evening news.

By announcing Russian intentions **in advance** of their actions, especially those involving deception, US intelligence has stayed ahead of Russian propaganda. Instead of controlling the story, Putin's head cheerleaders can do little more than bluster and complain.

Federal officials have warned that, like China, **Russia** is working online to **amplify divisions** ahead of the elections, but is not making up content this time around. Apparently, that's all being done here at home now.

In cyberspace, anyone can participate as a volunteer. In fact, both sides have enlisted online recruits to form **irregular guerrilla hacking militias**. Those sympathetic to Ukraine have been in particular urged to form an "**IT army**" for online operations, but Russia has its own **unpaid web warriors** as well.

With independent actors firing off **DDOS attacks** at will against not only Russia or Ukraine but their allies, the chance of serious unintended or collateral damage becomes very real. The war provides a ready patriotic smokescreen for criminal hackers, too.

The fog of war – that awful uncertainty that starts as soon as the first bullet is fired – is particularly thick in cyberspace. Attacks may come from any direction at any time, and attributing them properly is not at all easy.

Even as this is written, Russian hackers claim credit for **knocking election systems** offline in several states. It is very likely that more opportunistic attacks will happen before this is over, so users need firewalls, antivirus programs, backup and privacy tools.

SWCP will do our part, keeping watch and answering questions. Because like it or not, we are all in this mess together. Stay safe.

Correction – *Last issue, we referenced the "George Foreman murder" when we meant George Floyd. Apologies to all, and thanks to Marian, the Corrales librarian who spotted it – J.*