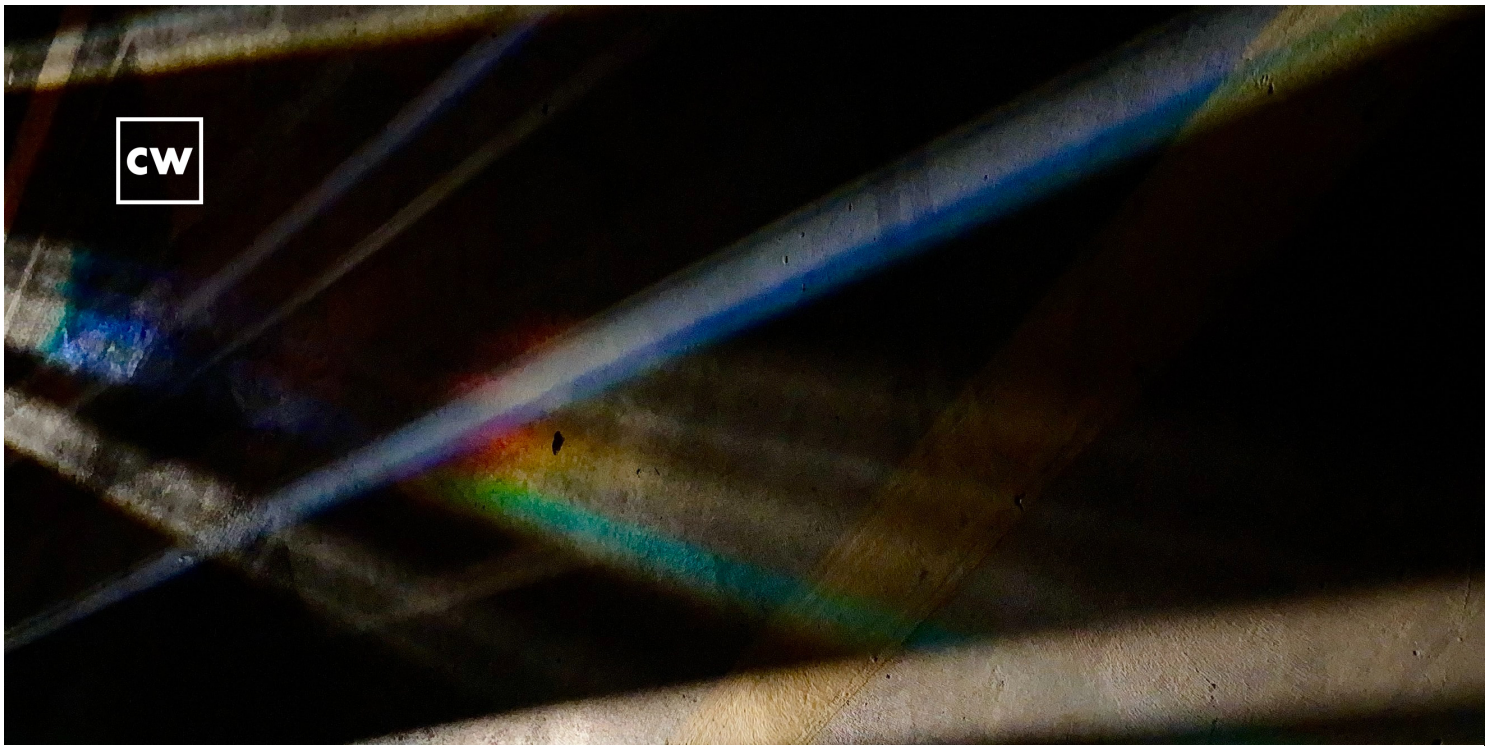
Spring 2-9-2023

After the war in Ukraine: Cyber revanchism

Jan Kallberg



By **Dr. Jan Kalberg** 1 hour ago

Wars eventually end. But when they do, especially if they end ambiguously, they give rise to lingering revanchism and preparation for the next round.

After the war in Ukraine: Cyber revanchism.

At some point in time, the war in Ukraine will end. How it will end is harder to forecast, but it will end.

Russia has taken a significant beating in the war; even if the Russian forces learned as the war progressed and partly mitigated the worst vulnerabilities, the war was not the intended success story it set out to be. The planned three days until the Ukrainian government collapsed and Ukraine could be absorbed into Russia never happened. Instead, it became a long war that made Russia look incapable, and less than a superpower.

The limited cyber exchanges during the conflict have surprised the cyber community as many expected far more cyber attacks and cyber campaigns to be executed at a time of war. So, will future peace be cyber peace as well? Probably not.

Here is the reason why. Russia historically has had a hard time dealing with defeat. There is a culturally entrenched will to strike back as any failure goes contrary to the spurious Russian perception of imperial grandeur and supremacy.

Revanchism, online.

The reason is simple. During the war, with sanctions and more questions asked in third- fourth-countries through which the harvest from the criminal activity is funneled, there is no business case. Cybercriminal networks need the ability to launder money in order to convert the stolen assets to such tangibles as gold, cash, apartments, cars, or whatever they want to buy. Under current sanctions, Russian cybercriminals face “hardship” in making these arrangements. Some of them have left the country to avoid being called up to the war in Ukraine, those still in the country cannot travel, and the outer world is more suspicious than before. Banks and financial institutions, even in developing countries, are concerned about breaking the sanctions and being punished, leading to an unwillingness to put profit before ethics. In the symbiotic relationship between the Russian cybercriminal networks and the security apparatus, some of the gangs might be pressed into service for the government as the war continues. Still, it is marginal compared to the cybercriminal activity driven by money.

Therefore, it is likely that after the war in Ukraine, we will see a general surge in ransomware, social engineering, and cyber attacks. Russia and its allies, who already harbor cybercriminal networks, would encourage these activities against Western countries as a form of digital revanchism.

These attacks don’t need to be at a grand national security level with strategic intent, because the cybercriminals want to squeeze out money, and the Russian regime wants the targeted societies to feel the pain. Consider the damage broad attacks can do, when they inflict individual pain: a ransomware attack that affected cars, for example, would leave drivers stuck with a car they can’t use unless they pay. David Brumley has envisioned ransomware locking up cars as one of his projections for 2023.

If you can't beat them, at least hurt them.

Revanchism in the face of defeat is nothing new. At the end of WWII, Germans attacked London with V-2 rockets which had no strategic or operational impact, but the Germans wanted to strike deep against the Allies even as their war went from bad to worse.

For the Russian leadership, to give their cyber criminal networks free range to attack Western interests, sheltered by the government and by Russian sovereignty, gives a sense of striking back. The Ukrainian war was not only defeat and mayhem, the Russians were able to bring the fight to the Western countries through unrestricted cyber attacks. In a Soviet manner, the Russians will likely claim having no knowledge or responsibility of the crescendo of cyber aggression even if it is blatantly obvious.

So do not rule out a larger cyber engagement after the war in Ukraine, rather than under the war, as it could be the cyber fallout of the conflict. A revanchist-in-spirit counter strike through proxies would be a face-saving way of getting in the last word.

(Jan Kallberg, Ph.D., LL.M., is an Assistant Professor in the Department of Mathematical Sciences at the United States Military Academy and a Scientist in the West Point Insider Threat Research Program. He is also a non-resident Senior Fellow with the Transatlantic Defense and Security program at the Center for European Policy Analysis (CEPA). Follow him at cyberdefense.com and @Cyberdefensecom. The views expressed are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of Defense, or the US Government.)